GNSS for Train Localisation Performance Evaluation and Verification

Von der Fakultät für Maschinenbau
der Technischen Universität Carolo-Wilhelmina zu Braunschweig

zur Erlangung der Würde

eines Doktor-Ingenieurs (Dr.-Ing.)

genehmigte Dissertation

von: Debiao Lu M.Sc.
aus: Nantong, Jiangsu, China

eingereicht am: 20.02.2014
mündliche Prüfung am: 17.06.2014

Gutachter: Prof. Dr.-Ing. Dr. h. c. mult. Eckehard Schnieder
Prof. Dr.-Ing. Jürgen Beyer

2014

"Measure what can be measured, and make measurable what cannot be measured."

Galileo Galilei

Acknowledgements

This dissertation is based on my research work in Institute for Traffic Safety and Automation Engineering (iVA) at TU Braunschweig in the last four years. Without the sincere support from many people, it would not have been written. I would like to express my gratitude to all the people who made this dissertation possible. Because of you, my research experience in Germany has become a story that I will always remember.

First, I owe my far deepest gratitude to my supervisor Prof. Dr.-Ing. Dr. h.c. mult. Eckehard Schnieder, who guided me into the rigorous and precise research world. He gave me not only the freedom to explore on my own, but also the structuralised methods to describe every concept clearly. This will be helpful for my whole life.

I would like to thank Prof. Dr.-Ing. Jürgen Beyer for the acceptance of co-supervising my dissertation. His intensive knowledge in GNSS helped me to establish a more stable ground for this dissertation. The constructive discussions and valuable comments are very useful for my further research.

I also would like to thank Prof. Dr.-Ing. Karsten Lemmer for hosting my doctor defence. He gave me useful suggestions for the defence in a preliminary talk.

All the colleagues at iVA are acknowledged for their contribution to an enjoyable working environment. I would like to extend a special gratitude to Federico Grasso Toro and Dirk Spiegel for giving corrections for this dissertation.

Furthermore I am very grateful to the Chinese Scholarship Council (CSC) to provide the scholarship for my research. This scholarship also gives me possibilities to extend the friendship with some Chinese friends from Beijing Jiaotong University.

Finally I would like to express my gratitude to my family. This dissertation is dedicated to my parents, Daoshan Lu and Yamin Wang, who decided 27 years ago to give birth to me as the second child in the family and supported me to go so far.

Braunschweig, 30.06.2014 Debiao Lu

Abstract

Global Navigation Satellite Systems (GNSS) are potentially applicable for various railway applications, especially the safety-related applications such as train localisation for the purpose of train control. In order to integrate GNSS for train localisation, a trustable stand-alone GNSS-based localisation unit should be developed. Then to comply with EN 50126 (reliability, availability, maintainability, and safety; RAMS) standards, the demonstration of GNSS quality of service (QoS) should be evaluated in consistent with RAMS. However there are currently no appropriate performance evaluation methods on GNSS for railway safety-related applications.

This dissertation identifies the required performance for train localisation in consideration of GNSS QoS and railway RAMS. The common and different properties of the performance are analysed in detail using consistent attribute hierarchy structures based on UML class diagram. Then formalised performance requirements are proposed quantitatively on four properties (accuracy, reliability, availability, and safety integrity). After that, the evaluation and verification methodologies are introduced. The evaluation methodology is using a reference measurement system for GNSS receiver measured train location accuracy identification, and a stochastic Petri net (SPN) model for GNSS receiver measured train location accuracy categorisation. The SPN model illustrates the GNSS receiver measured train locations into three states (up state, degraded state, and faulty state). Then the four proposed properties are allocated and estimated formally using the three states in the SPN model. The verification methodology is used to verify the GNSS receiver measured train location in real time based on a localisation unit. The GNSS receiver measured train locations are verified using hypothesis testing methods based on the accurate digital track map provided beforehand. Then train location estimation from the localisation unit is verified according to the mileage of the train. With the verified train location estimation from the localisation unit, the corresponding safety margin for each train location is calculated.

The data for evaluation and verification methodologies are collected from a test train running on a railway track in High Tatra Mountains. The results show an approach of the possible certification procedure for the GNSS receivers in railway safety-related applications.

Kurzfassung

Globales Satellitennavigationssystem (GNSS) können für verschiedene Anwendungen im Schienenverkehr, vor allem für sicherheitsrelevante Anwendungen wie Zugortung zum Zweck der Zugsicherung gestützt werden. Um GNSS für Zugortung zu integrieren, muss eine eigenständige satellitenbasierte Ortungseinheit entwickelt werden. Um die Entwicklung in Einklang mit EN 50126 (Überlebensfähigkeit, Verfügbarkeit, Instandhaltbarkeit, und Sicherheit; RAMS) durchzuführen, muss der Nachweis der Güte von GNSS (Quality of Service; QoS) entsprechend in Einklang mit dieser Norm bewertet werden. Allerdings gibt es zurzeit keine RAMS Bewertungsverfahren für satellitenbasierte sicherheitsrelevante Anwendungen im Schienenverkehr.

Diese Dissertation identifiziert die notwendigen Anforderungen für die Zugortung unter Berücksichtigung der Güte von GNSS und den bestehenden Normen bezüglich RAMS im Schienenverkehr. Die gemeinsamen und unterschiedlichen Eigenschaften der Anforderungen werden detailliert mit Nutzung einer Attributhierarchie basierend auf UML-Klassendiagrammen dargestellt. Danach werden formalisierte Leistungsanforderungen quantitativ für vier Eigenschaften (Genauigkeit, Zuverlässigkeit, Verfügbarkeit und Sicherheitsintegrität) vorgeschlagen. Darauf aufbauend werden die Bewertungs- und Verifikations- Methoden eingeführt. Die Bewertungsmethode nutzt ein Referenzmesssystem zur Identifikation der Zugortungsgenauigkeit der GNSS Empfänger und ein stochastischen Petri-Netz-Modell (SPN-Modell) für die Kategorisierung der GNSS Empfänger Zugortmessungen. Das SPN-Modell veranschaulicht die GNSS Empfänger Zugortmessungen in drei Zuständen (up state, degraded state, faulty state). Dann werden die vier vorgeschlagenen Eigenschaften zugeordnet und formal mit Nutzung der drei Zustände im SPN-Modell geschätzt. Die Verifikationsmethode wird verwendet, um die GNSS Empfänger Zugortmessungen in Echtzeit zu verifizieren. Die GNSS Empfänger Zugortmessungen werden mit einer Hypothesentestmethode auf der Grundlage der genauen digitalen Streckenkarte verifiziert. Mit der verifizierten geschätzten Zugortmessung wird der resultierende Sicherheitsbereich für jeden Zugort berechnet.

Die Daten für die Auswertungs- und Verifikationsmethoden wurden von einem Zug im Regelbetrieb auf einer Eisenbahnstrecke in der Hohen Tatra gesammelt. Die Ergebnisse dieser Arbeit zeigen einen Ansatz der möglichen Zertifizierungsverfahren für die GNSS-Empfänger für sicherheitsrelevante Anwendungen im Schienenverkehr.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The first navigation satellite was launched into space in 1978 by the **U**nited **S**tates of **A**merica (USA) as part of the **G**lobal **P**ositioning **S**ystem (GPS), then in 1993 GPS reached its **I**nitial **O**peration **C**apability (IOC). Three years later in 1996 **Glo**balnaya **Na**vigatsionnaya **S**putnikovaya **S**istema (GLONASS) also reached its IOC. In the 21st century, both **E**uropean **U**nion (EU) and China are launching navigation satellites for their Galileo and **B**ei**D**ou Navigation Satellite **S**ystem (BDS) to provide similar functions and performances like GPS and GLONASS. These four systems and the upcoming satellite-based localisation systems are summarised as **G**lobal **N**avigation **S**atellite **S**ystems (GNSS). A brief history and expectation of GNSS satellite numbers for the four navigation systems are shown in Figure 1.1.

BDS has formally commenced regional operations on 27 December 2012 [1]. Galileo is in its **I**n-**O**rbit **V**alidation (IOV) phase since 12 October 2012 [2]. This IOV phase is as the fundamental phase when the European navigation system really goes from theory to practice, both the satellites and the supporting ground stations working together and being checked in real time [2]. So up to now there are more than 70 navigation satellites over the sky. As expected there will be over 120 navigation satellites in 2020 [3]. A short summary of number of satellites for four GNSS in 2013 and prediction in 2020 is shown in Table 1.1.

GNSS provide the capability for determining the time, location, and velocity. These huge number of GNSS satellites will provide more satellites for these three capabilities thus improving the performance of the GNSS in general. This also brings more chances for emerging applications, such as safety-related applications in transportation. In the design phase of Galileo, the **S**afety **o**f **L**ife (SoL) service was designed as an elementary service thus distinguishing it from other three GNSS [4]. But later, this plan was cancelled, since SoL service has been implemented by

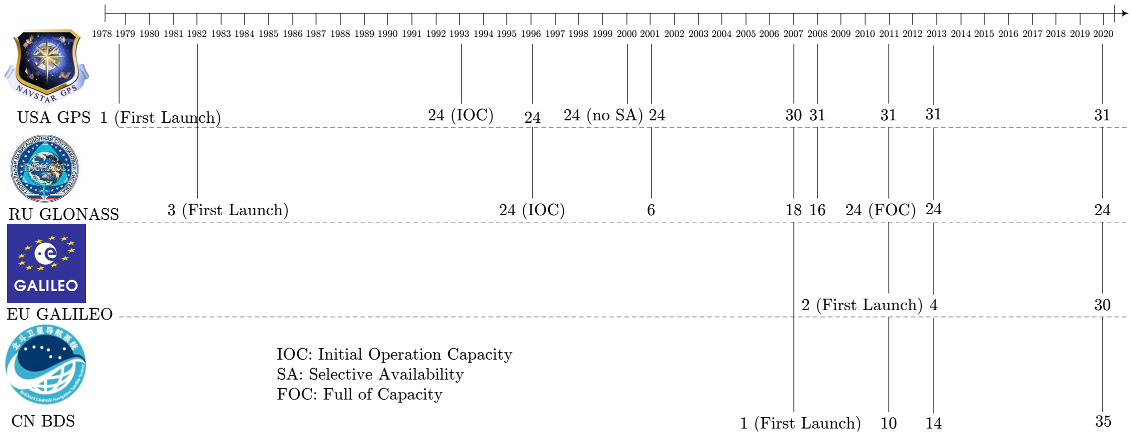


FIGURE 1.1: GNSS Satellite Number History and Expectation

TABLE 1.1: Satellite Numbers of Each GNSS in Operation and Expectation

GNSS	Satellites in Operation (2013)	Satellites in Expectation (2020)
GPS	31	31
GLONASS	24	24
Galileo	4	30
BDS	14	36
Sum	73	121

European **G**eostationary **N**avigation **O**verlay **S**ervice (EGNOS) since March 2011. The EGNOS SoL service is provided openly and is freely accessible without any direct charge and is tailored to safety-related transport applications in various domains, the use of the EGNOS SoL service may require specific authorisation by the relevant authorities in the application sectors concerned [5].

In surface transportation, especially in railway domain, GNSS can be applied in many applications, for example the safety-related railway signalling systems. The railway signalling systems are providing essential traffic management and traffic control information for both passenger trains and freight trains in the network. One of the important issues of railway signalling is to locate the train as accurate as possible through train detection and train localisation techniques. The full range of train detection and localisation functions may include proving the absence of a train, proving the presence of a train, and (directly or indirectly) measuring or indicating the velocity of a train [6]. The European railway calls for harmonised train control systems, **E**uropean **R**ail **T**raffic **M**anagement **S**ystem (ERTMS)/**E**uropean **T**rain **C**ontrol **S**ystem (ETCS) came from an EU directive in 1991 [7]. ETCS is specified at four levels, with the ETCS-3 (Level 3) it goes beyond the pure train protection functionality with the implementation of full radio-based train spacing called moving block [8]. The **R**adio **B**lock **C**entre (RBC) needs to receive the vital information via **G**lobal **S**ystem for **M**obile Communications for **R**ailway (GSM-R) such as the train location [9]. GNSS receiver is exactly at the place to deliver train location. To integrate GNSS into the railway signalling systems, GNSS receiver can be installed on the train as part of the train **O**n-**B**oard **U**nit (OBU), and then GNSS receiver is treated as an instance performing train localisation function. The OBU should report the location of the train regularly to the **T**rain **C**ontrol **C**entre (TCC) in accordance with the requirements, local laws, and regulations [10] [11]. However, GNSS receivers are currently neither standardised nor certified for train localisation purpose.

Since the birth of railway, there are safety specifications for train operation and managements. Currently, there are many national, regional, and international safety standards. For example, the safety standard and safety targets for general electronic devices published by **I**nternational **E**lectrotechnical **C**ommission (IEC) as an international standard called IEC 61508 [12] [13] [14] [15] [16] [17]. And there are also railway specific safety-related application standards published by **C**omité **E**uropéen de **N**ormalisation **Élec**trotechnique (CENELEC) as a regional standard for Europe. The CENELEC EN 50126 concerns demonstrating the performance of railway signalling system [18]; CENELEC EN 50128 concentrates on the methods needed to provide software which meets the demands for safety integrity [19]; and CENELEC EN 50129 addresses the approval process for individual systems which may exist within the overall railway control and protection system [20]. These standards are also published by **D**eutsches **I**nstitut für **N**ormung (DIN) as national standards. All the standards introduced above are used accordingly for over 10 years. Any new devices or equipments performing safety-related functions should obey the standards. So the implementation of GNSS for train localisation should also obey the stands mentioned above [10] [21].

1.1 Purpose of the Dissertation

The purpose of this dissertation is to show how to trust the performance of GNSS for train localisation. This requires a clear understanding of the properties of the performance. This also requires GNSS for train localisation to conform the related standards, specifications, and advisories, thus brings a certifiable GNSS-based localisation unit to be applied for train localisation. This purpose can be decomposed into three objectives.

The first objective is the formal definition and migration of "GNSS for train localisation performance" properties with the consideration of both GNSS **Q**uality **o**f **S**ervice (QoS) performance properties [22] and railway RAMS performance properties [18]. The migration process uses the terminologies of dependability engineering and safety engineering in both GNSS and railway applications. The definition and migration of GNSS for train localisation performance properties in a formal structural way is the foundation to answer "What is the performance?" and "How to trust?", and yet, not done by any others.[1]

The second objective is the quantitative evaluation of the properties resulting from the achieved first objective. This objective is aiming to answer the question: "What is the performance?" The performance evaluation requires the help of a train location reference measurement system. The reference system together with the GNSS receiver generates the train location at the same timestamp, the deviation between GNSS receiver and reference locations are quantified through stochastic analysis. The performance of GNSS receiver measured train location is quantified according to the definition of the properties. Then the quantified performance is identified according to the performance specifications.

The third objective is the acceptance of the GNSS receiver train location by real-time verification. This objective is to answer the question "How can we trust?". This calls for other localisation sensors together with GNSS receiver composing a GNSS-based train localisation unit. The design of the localisation unit helps to execute the verification process by redundancy and voting schemes. The verification process also uses the identified performance values as the basic knowledge of the GNSS performance. Then, the acceptance of train location decision is made.

These three objectives can be attributed to different phases of the system lifecycle. The three objectives as migration, evaluation, and verification can be shown in a complete process in Figure 1.2.

In order to evaluate the train location measured by GNSS receiver, a reference measurement system is used as an external resource. Then in the real-time verification of the train location measured by the GNSS receiver, there is no reference measurement system anymore. The GNSS-based localisation unit is using its internal resources to decide the acceptance of GNSS receiver measured train location. So these two objectives differs each other from many aspects as shown in Table 1.2.

[1] The structralised performance properties intended in GNSS for train localisation is not raised by any others. Based on this, the performance values in a medium density railway line is also not calculated by any others.

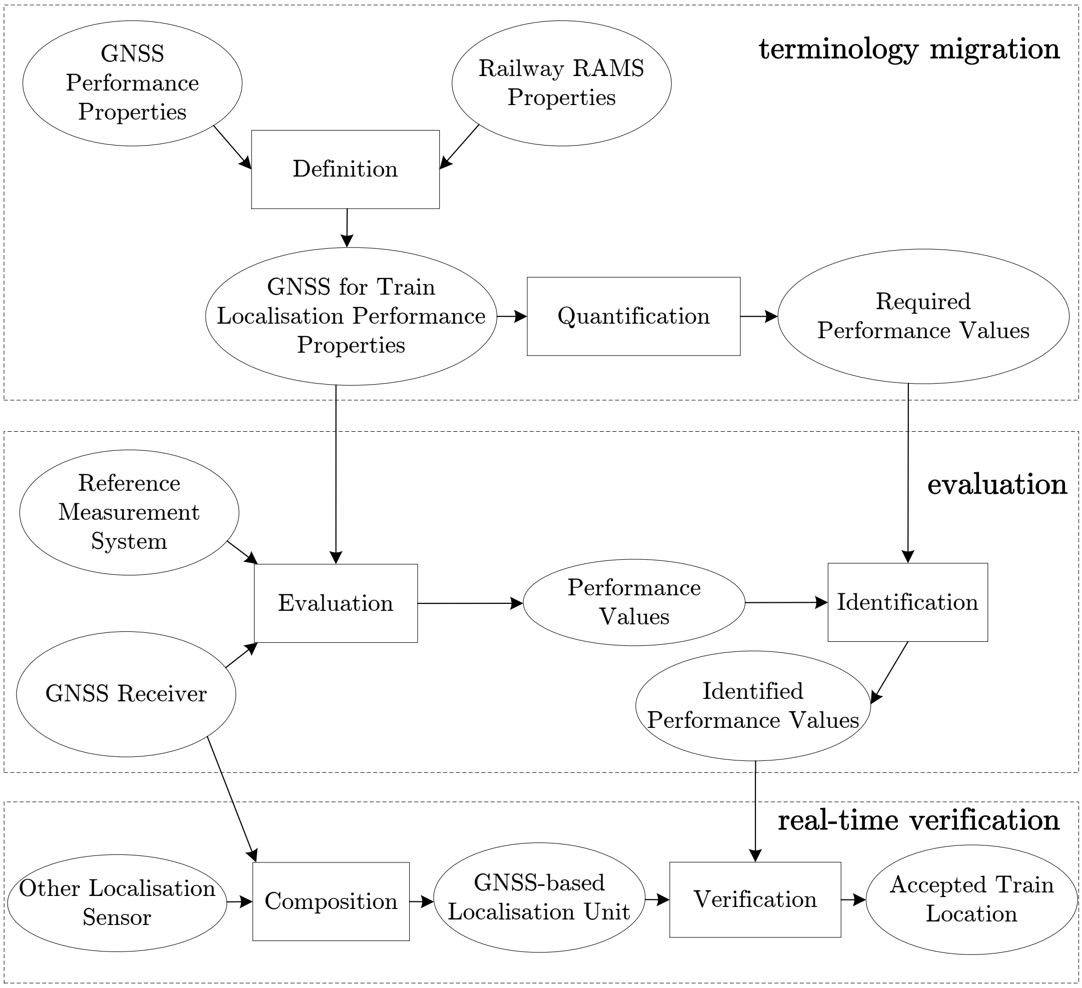


FIGURE 1.2: Three Objectives and Relations of the Dissertation

The external evaluation is the foundation for the real-time internal operation. This brings the system from design phase to operation phase.

The terminology migration is to analyse the GNSS performance properties and the railway RAMS properties. During the definition of the properties, the common and necessary properties of GNSS for train localisation performance is migrated. The migrated performance properties sets the direction for the performance evaluation. The evaluation results also calls for quantitative values, the GNSS for train localisation performance properties are also quantified according to the requirements from GNSS performance and railway RAMS as performance specifications.

The evaluation is using the reference measurement system together to deliver the train location from both sides. The GNSS receiver measured train location and the reference measured train location are generated, then the time for the locations is matched. The analysis results show the performance in values and units. The performance values can be identified with the specification as the identified performance

Table 1.2: Evaluation and Verification in Comparison

Objective	GNSS receiver with stand-alone reference measurement system for evaluation	GNSS receiver inside a GNSS-based localisation unit for real-time operation
Architecture	two independent systems	multi-sensor, redundant
Function	evaluation	verification
Data Usage	macro study	micro study
Reference	external	internal
Phase	design	operation

values. This shows the understanding of the performance both in properties and values. The process of the evaluation requires the clear definition of the evaluation process to reproduce the performance values again.

The real-time verification of the train location is the micro study of the GNSS receiver measurements. The successful micro study of the GNSS performance is based on the macro study of it. The macro study evaluates performance values. The evaluation is using a complete stand-alone reference system, but the verification is involving another localisation sensor together as internal source building a GNSS-based localisation unit. The verification process is using the evaluated and identified performance values as characteristic values for the micro study. This brings the acceptance of the train location measurements.

So, the train location measurement can be finally trusted which answers the questions proposes at the beginning. The whole process shown in Figure 1.2 also leads naturally to the structure of the dissertation in Section 1.2.

1.2 Structure of the Dissertation

The dissertation consists of 8 chapters, including both methodologies and numerical analysis results from the previous experiments to support the methodologies. From Chapter 5 to Chapter 7 are my original personal work: establish the appropriate GNSS for train localisation performance properties; establish a certifiable process for the evaluation of the GNSS for train localisation performance properties; and finally a real-time verification process based on the identified performance values from the evaluation process.

Chapter 1 describes the purpose of the dissertation and the structure of it.

Chapter 2 investigates the state of the art of GNSS for train localisation. A short history of train detection and localisation is introduced as the background. After that both research projects and real application instances for GNSS-based train localisation and train operation are presented. With this background, the evaluation and verification research statuses on GNSS for train localisation and related topics are introduced.

Chapter 3 describes the methodologies used in this dissertation. The **U**nified **M**odeling **L**anguage (UML) basic theory and implication for UML in figures are introduced. Based on that, the attribute hierarchy for clarifying the concepts and terms is established. With the clear understanding of the terms, the possibility and statistics theory for evaluation purposes are presented. The distributions used in this dissertation are also mathematically illustrated. In order to formulate the terms for the following evaluation and verification properties formally, the Petri net and further the stochastic Petri net are both stated from the formal side viewpoint. The optimal detection theory is also interpreted for verification purposes.

Chapter 4 illustrates the three systems in this dissertation: GNSS receiver, reference measurement system, and GNSS-based localisation unit. With the clear understanding of the different aspects of the systems, the GNSS receiver localisation principles are introduced as the background of the whole process. The environmental effects of measurement accuracy are analysed based on the localisation principles. Then the GNSS performance requirements from both the service provider side and the user side are introduced separately. Starting from Chapter 5 to Chapter 7, the dissertation goes through the formal migration, performance evaluation and then real-time verification step by step.

Chapter 5 depicts the migration of GNSS performance properties to railway train localisation. The GNSS performance requirements introduced in Chapter 4 are analysed in detail. The relation between the GNSS performance properties, and the relation between the GNSS RAMS are analysed both internally and externally. The UML class diagram modelled terms and the relation between them are analysed. Then the appropriate properties are raised formally. With the properties and the attribute hierarchy of the properties, a specification inherited from the GNSS performance requirements is raised.

Chapter 6 is going into detail about performance evaluation. Firstly, based on the accuracy evaluation, a stochastic Petri net model interpreting the measurement states is built for formal evaluation of the properties proposed in Chapter 5. Secondly, general accuracy performance of GNSS for train localisation is evaluated as a basis, then the reliability and availability are evaluated based on the accuracy performance values. Finally, different environments are analysed for the safety integrity property, GNSS parameters such as number of visible satellites and **D**ilution **O**f **P**recision (DOP) are inputs for the evaluation. Two environmental scenarios are investigated with the consideration of both safe and dangerous failures of GNSS for train localisation and the corresponding safety integrity level. The data collected in the High Tatra Mountains is shown as the numerical results from the evaluation methodology.

Chapter 7 introduces the necessity of operation without reference measurement system for real-time verification of the GNSS receiver measured train location. Then the optimal detection methods are applied to decide the GNSS receiver measured train locations are acceptable as on the track or not. And then a safe two layer 2oo2 structure is introduced for failure diagnosis and elimination for the GNSS-based localisation unit. The dangerous undetected and detected failures are analysed as part of the verification methodology. The numerical results are shown to present the verification algorithm performance.

With the methodologies and numerical results, the conclusions in Chapter 8 are made on GNSS for train localisation both evaluation and verification. Then the evaluation methodology is generalised as a universal approach to quantify the performance of other sensors in consideration of a certifiable process of the sensors for safety-related applications according to standards. Besides, further possible research topics are recommended.

The whole structure of the dissertation is shown in Figure 1.3.

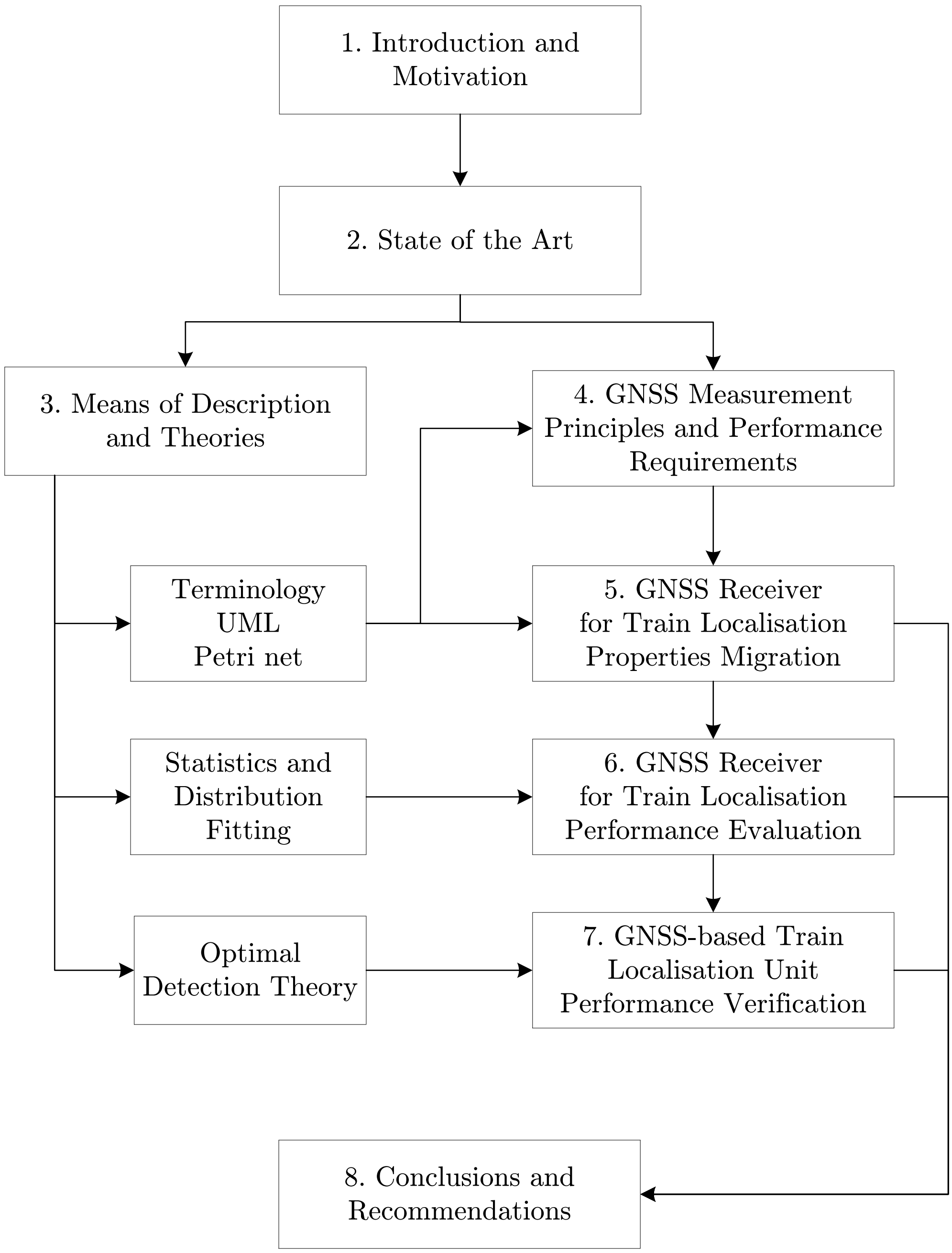


FIGURE 1.3: Structure of the Dissertation

Chapter 2

State of the Art

It may seem obvious, but to control the route of the trains on a rail network, train location and velocity information are essential. It is a problem since the railway was invented, many researchers are always devoted to find more advanced solutions[2].

2.1 Train Detection and Localisation Methods in Railway

In the early days of railways, the train location information was collected by and passed between humans [6]. Long time after that, they began to use electric energy to detect the trains, the first recorded use of which was in Turner, New York, in 1851 [23]. And then in 1872, the failsafe track circuit was invented by William Robinson [23]. At that time, track circuit was recognised as the key element for the automatic train control. As train velocities and traffic densities rise the risks and consequences of a failure of the train detection system become more acute, more advanced technologies are used for train detection such as axle counter, Balise, light cable, etc. [23] [24] [25]

There are two different approaches to get the train location information. One is traditional train detection, they are devices like track circuit, axle counter, passive and positive balise, etc. All of them need to be installed along the track, the accuracy of the train location depends on the length or the distance of the adjacent two units. The other is train localisation, they are odometer, inertial sensor, Doppler radar, **E**ddy **C**urrent **S**ensor (ECS) [26] and also the instance to be investigated in this dissertation - GNSS. They are basically communication based approaches, the sensors are installed on the train, the train transmits its location to TCC.

[2] The information about the researchers is introduced in the following sections of this chapter.

Table 2.1: Comparison of Train Detection and Localisation Sensors

Sensor	Category	Cost	Accuracy
track circuit [27]	detection	high	same as track circuit length
axel counter [28]	detection	high	same as the length between two axel counters
balise [29]	detection	high	same as the length between balises
odometer [30]	localisation	low	accumulated errors with time and distance
inertial sensor [31]	localisation	high	accumulated errors with time and distance (only when the vehicle is moving)
Doppler radar [32]	localisation	high	accumulated errors with time and distance, mainly used for velocity measurement (also significant noise in the signal)
ECS [26]	localisation	low	mainly used for velocity calculation and switch recognition, accuracy related to the accuracy of the switch database
GNSS receiver [33]	localisation	low	error varies according to satellite constellations, environments, location and velocity measurements are independent

The TCC then uses this location data to issue authorities to each train to permit further safe movement. The train location may be determined by combinations of the sensors stated above. A major benefit of the communications based approach is that it removes equipments from track. Since the equipments are installed on the train, they can provide more flexible and accurate location. This will increase the capacity of the system by reducing the block section boundary. A rough comparison of the accuracy and cost of all the mentioned technologies for train detection and localisation sensors and equipments is shown in Table 2.1.

With the comparison stated in Table 2.1, the accuracy of GNSS receiver measured locations change in different environments and also have relation to the satellite geometry. The general accuracy of GNSS receiver measured location needs to be evaluated along railway tracks. Because of the low cost and the ability of getting rid of track side equipments, the GNSS-based train localisation is a promising instance as part of the OBU for the railway signalling system.

2.2 GNSS for Train Localisation Researches and Applications

Since the IOC of GPS, it has been actively involved in aviation applications. The surface transportation has also been a hot field only years after that. Aspects of

Table 2.2: European Projects on GNSS for Train Localisation

Project Name	Period	System	Funding	Goal
APOLO [34]	1999-2001	GPS	FP5	test the base element of GPS for train localisation
LOCOPROL [35]	2001-2004	GPS	FP5	for low density lines, extend the ERTMS train protection systems
LOCOLOC [36]	2002-2004	GPS	ESA	development of a complete low cost fail-safe train navigation and integrity system based on GNSS, service centre for LOCOPROL
INTEGRAIL [37]	2001-2004	EGNOS	ESA	EGNOS signal in safety-critical railway traffic management and control, provide reliable location and integrity information under varying operational conditions
GADEROS [38]	2001-2004	Galileo	FP5	perform tests on a number of prototypes on a low traffic line within ERTMS/ETCS
ECORAIL [39]	2001-2005	GNSS	ESA	integration of GNSS into safety critical railway applications
RUNE [40]	2001-2006	GNSS	ESA	GNSS as a virtual balise, safety application with EGNOS
GEORAIL [41]	2004-2008	none	UIC	guidelines for the application of CNTD for train localisation
GRAIL-1 [42]	2005-2008	GNSS	FP6	a common specification for the GNSS subsystem at different levels of ERTMS/ETCS architecture
GRAIL-2 [43]	2010-2012	GNSS	GSA	to define, develop and validate a GNSS-based Enhanced Odometry (ETCS) application in high speed railway lines
GaLoROI [44]	2012-2013	Galileo	FP7	develop a certifiable safety relevant satellite based localisation unit for low density railway lines
EATS [45]	2012-2016	Galileo	FP7	a model of the complete on-board ERTMS system behaviour to eliminate interpretation differences

high meteorological quality as well as safety relevance of the GNSS-based train localisation have been focused equally.

2.2.1 GNSS for Train Localisation Research Projects

Starting from 1999, there have been a lot of research projects in GNSS for train localisation. The **A**dvanced **Po**sition **Lo**cator (APOLO) project was at the very beginning of attempt for bringing GNSS into railway signalling system. After that, there are many research projects under EU **F**ramework **P**rogramme (FP)s or supported by **E**uropean **S**pace **A**gency (ESA). Table 2.2 shows the research projects in Europe aiming at GNSS into train localisation.

The projects in Table 2.2 are trying to introduce the prototype and the specifications at the early stages, including application in railway specific scenario such as level crossing in ECORAIL, and integrated localisation unit such as in INTEGRAIL. Later the project GEORAIL by UIC, is aiming at providing the guideline for the track map structure for railway domain, called **C**oordinate based continuous **N**umerical **T**rack **D**escription (CNTD). The GaLoROI project is going to introduce a localisation unit and a complete safety process dealing with safety cases for the localisation unit. A systematic evaluation and verification of GNSS for train localisation is on demand.

2.2.2 GNSS for Train Localisation Researches at iVA

Scientific research of location measurement performance for surface vehicles has been a central and systematic work of the Institute of Traffic Safety and Automation Engineering (iVA) at TU Braunschweig. For the train localisation part, Table 2.3 shows the dissertations working on localisation unit, the performance of GNSS, the performance of the localisation unit in a time sequence.

The research started from establishing a GNSS-based localisation unit, then analysing the performance of the localisation unit. In order to quantify the performance of GNSS receiver, a reference measurement system to validate the GNSS receiver performance was built. The measurement accuracy and reliability of the reference measurement system and the GNSS receiver is the topic then. Now the research topic upgrades to the standardised process for GNSS receiver performance qualification.

2.2.3 GNSS for Train Localisation Applications

Not only the academic institutes are investigating possible integrations of GNSS for railway applications, the industry companies have also implemented GNSS for

Table 2.3: Train Localisation Related Dissertations of iVA at TU Braunschweig

Name	Year	Category	Goal
Kiriczi [46]	1996	localisation QoS	safe localisation with fault diagnose
Leinhos [25]	1996	localisation unit & QoS	localisation unit architecture
Klinge [47]	1997	localisation unit	localisation platform
Bikker [48] [49]	2002	localisation unit	reference measurement system
Poliak [50]	2007	localisation unit & QoS	reference measurement system and validation of GNSS
Hänsel [51]	2008	localisation unit	certification process of GNSS after technical standards
Wegener [52]	2014	localisation QoS	measurement uncertainty of GNSS in dynamic measurements
Lu	2014	localisation unit & QoS	QoS evaluation for a certifiable process and localisation unit structure

train localisation in some lines. The following is a list of GNSS for train localisation applications on some lines.

- Integrated Train Protection System (KLUB-U)

KLUB-U was implemented in Russia using satellite based localisation in 2010 near Sochi, Russia [53]. The system determines train movement qualitative values (coordinates, speed) by the data from satellite navigation devices, the digital track map of a railway section and distance-and-speed sensors/meters, which are installed on a wheel-set journal box [54]. Different issues shall be addressed by this modern train control system. This is on the one hand the low visibility of signals at difficult environmental conditions like fog, rain and snow, on the other hand the targeted high speeds where driving at sight to signals is not possible. This technology still needs to be improved for extreme environments.

- **I**ncremental **T**rain **C**ontrol **S**ystem (ITCS)

The ITCS has been implemented in USA for **P**ositive **T**rain **C**ontrol (PTC) purposes. ITCS consists of three main components - communication network, wayside component, and on-board component. The wayside component for ITCS is an overlay on existing signalling system, it reports in a conventional way. And the on-board component uses a vital location determination system, based either on balises or GPS, to locate the train and an on-board database to determine the relative location of all features of the railroad such as signals, switches, and crossings [55].

ITCS has been applied on the Michigan corridor line between Detroit and Chicago since 2000. ITCS in Michigan is a fail-safe (vital) positive train control system that overlays the existing signal system for improved safety and provides a cost-effective solution for high-speed train operation. ITCS has also been applied in Qinghai-Tibet railway line in China. Because of the harsh environment of this new railroad (5,000 meters at its peak with track laid over permafrost), the traditional signalling system was not installed [56]. This system is also under construction in Nigeria by the railway company Eko Rail since 2011 [57]. Besides, the system is also under construction in Australia from 2011, this line will be operated by Fortescue Metals Group [58].

- Signalised Train Control (ZLB STH)

ZugLeitBetrieb (Signalised Train Control) is a satellite based train control system developed by the University of Applied Sciences Upper Austria and operated by Stern & Hafferl [59]. The trains equipped with the signalling system have an on-board unit including a device for the driver as well as a GPS receiver. This unit communicates through a data radio system with the work-place for a train controller which is responsible for the movement authority for the trains. Spring switches make sure that train meetings in stations do not lead to accidents because this type of switches allow only driving on one specific switch in stations from one direction. In case the satellite based localisation is not operational, radio communication is used as fallback option [60].

- Satellite-based Operation and Management of Local Low Traffic Lines (SATLOC)

The SATLOC project is funded by the European Commission in the FP7 program. a railway line in Romania shall be equipped with satellite based localisation technology. The 28 kilometres long demonstration line from Braşov to Zărneşti is located in the Romanian region of Transylvania and is operated by the private Romanian company Regiotrans. The target of SATLOC is to prove the applicability of GNSS for ERTMS/ETCS level 3. The application contributes to the adoption of EGNOS in rail primary safety and paves the way to the introduction of Galileo in the railway safety domain. The ERTMS Regional will directly benefit from this line [61].

As seen from the three train control systems and one still in development, they are different technologies but all using GNSS performing the main localisation function and also obeying the safety requirements. The Figure 2.1 shows the mentioned GNSS-based railway operation and train control systems according to the geographical locations of them. These technologies are only applied on several pilot lines. The first three technologies are all having a fall back system to keep them as safe train control systems. The complete safety evaluation and verification process are still waiting to be performed.

FIGURE 2.1: GNSS-based Train Control Systems in Operation

2.3 Migration of GNSS QoS and Railway RAMS

GPS is already standardised and then applied for civil aviation applications, such as en-route, **A**pproach **P**rocedure with **V**ertical guidance (APV), etc. From a more general viewpoint, GNSS is also freely available to surface transportation, such as automobiles and locomotives.

The safety concept of railway has a significant difference from aviation one. Firstly, the aviation domain uses "integrity", while the railway domain uses "safety". The definitions and differences of both terms will be illustrated in Chapter 5. Secondly, the aviation domain normally concerns both horizontal and vertical accuracies, railway domain concerns more horizontal accuracy. Thirdly, the aviation domain has its own definition of GNSS in precise approaching applications for risk acceptance by per approach (one approach is 150 seconds), the railway society normally defines the hazard rate in the time span of one hour.

GNSS avionic standards are international standards. For example, the **S**tandards **A**nd **R**ecommended **P**ractice**s** (SARPs) were first adopted by **I**nternational **C**ivil **A**viation **O**rganisation (ICAO) in 2001, then subsequently amended 11 times [62]. Aviation has been not only using stand-alone GNSS navigation, but also using **S**pace **B**ased **A**ugmentation **S**ystem (SBAS) and **G**round **B**ased **A**ugmentation

System (GBAS) accordingly. SBAS and GBAS provide integrity in a multi-step procedure laid out in **R**adio **T**echnical **C**ommission for **A**eronautics (RTCA) **M**inimum **O**perational **P**erformance **S**tandards (MOPS). They are RTCA DO-208 for airborne supplemental navigation equipment using GPS [63], RTCA DO-229D for **W**ide **A**rea **A**ugmentation **S**ystem (WAAS) [64], and RTCA DO-253C for **L**ocal **A**rea **A**ugmentation **S**ystem (LAAS) [65]. These systems indicate which ranging measurements should be excluded as unsafe to use and providing bounding error standard deviations for the remaining usable measurements. There are several researchers trying to make a appropriate migration of GNSS QoS into surface transportation, as illustrated as follows.

Sam Pullen from Standford WAAS lab differentiates the aviation "specific risk" and non-aviation "average risk". The "average risk" is the foundation for **P**robabilistic **R**isk **A**ssessment (PRA) in non-aviation applications. The research results show several means to migrate the "specific risk" requirements from SBAS and GBAS for non-aviation users. The results indicates smaller error bounds and improved availability for non-aviation applications [66]. The work, which is generally for non-aviation users, is not directly applicable in railway applications since in railway there already exists standards for risk assessment of the equipment or software for railway safety-related applications.

Aleš Filip and Julie Beugin have presented an interpretation of Galileo SoL service requirements corresponding to railway **R**eliability, **A**vailability, **M**aintainability, **S**afety (RAMS). They introduce the relation of reliability, availability, and safety in a "pyramid", then illustrate the probability of failure allocation into the "pyramid" [67] [68] [69]. Their work provided a method to migrate the existing EGNOS requirement for aviation into railway using Markov chain based process. But a more formal migration is required for it from concept, qualitative, and also quantitative representation.

In this dissertation, the GNSS performance requirements for train localisation are defined consistently after comparing the requirements in GNSS, avionic and railway standards, and appropriate GNSS for train localisation performance properties are migrated, then the values and the units of each property are formally proposed.

2.4 Evaluation of GNSS Receiver for Train Localisation Performance

The research applications of GNSS for train localisation has been shown by Table 2.2 and Figure 2.1 above. The most demanding work is the standardisation and certification of GNSS localisation in railway safety-related applications. GNSS receiver measured location is sensible to the environments along the track as mentioned in Table 2.1. In order to have a complete understanding of GNSS receiver measured train location performance for railway signalling systems, it is both necessary and important to test the GNSS for train localisation on existing railway tracks, and then find the rules behind GNSS for train localisation performances in certain railway environmental scenarios. For each identified environmental scenario, the GNSS for train localisation performance needs to be evaluated and then verified as a general statement for this kind of environment.

It is true that GNSS receivers are expected to operate under railway environment conditions. The practicalities of testing how a GNSS receiver deals with the real environmental scenarios will be very difficult. The test setup will be unwieldy as it would be necessary to isolate and quantify all the GNSS signals reaching the receiver as well as assessing its own response to the signals. And the necessity to test the GNSS receiver with a representative sample of different multipath and other effects would make the process both long-winded and open to a myriad of uncertainty. As a matter of fact, there are several standards and procedures for evaluating GNSS for train localisation in a more general performance [70]. But actually for GNSS in safety-related applications in aviation, the environmental situations are much easier to deal with than railways. When a plane is in en-route mode, the multipath and shadowing problem are not a problem. The environmental scenarios affecting the accuracy performance in aviation is approaching with vertical guidance phase. It is quite different from GNSS for surface transportation applications. In surface transportation, the multipath and other affects will affect GNSS performance almost everywhere. There are only a handful of people doing research on evaluating GNSS performances in railway requirements [49] [50] [71] [72] [73].

Aleš Filip has been trying to applying SoL services of Galileo/EGNOS to railway localisation. The different performance requirements set up by EGNOS are analysed and the one fits for railway applications is determined. Based on this, the EGNOS data are evaluated on this purpose [71] [72]. This sets up a first example for evaluating GNSS performances for railway application purpose.

Julie Beugin and Juliette Marais have been doing evaluation of GNSS in railway performances by simulation methods [73]. The availability and reliability aspects of different environmental scenarios are analysed, but safety is still not stated.

Gert Bikker describes the basic possibilities of reference measurement systems for GNSS applications in railway traffic and gives an outline of it and then explains one of the first approaches [49]. This provides a solid background for the evaluation of the necessary properties of GNSS for train localisation. Then Jan Poliak shows the validation method of GNSS for railway applications using the reference measurement system [50].

For evaluation purpose, the formal method is also required for safety-related applications. In this dissertation, a stochastic Petri net model for GNSS receiver performance evaluation is built, and the safety issues are analysed for two environmental scenarios.

2.5 Verification of GNSS-based Localisation Unit Performance

The evaluation of GNSS receiver for train localisation performances is the basis for any further realisation and the ruler for hazard analysis and risk assessment on GNSS for train localisation. So the purpose of verifying the performance of GNSS in real time is requested. The verification includes diagnostic of the GNSS receiver measured train location. Basically, the verification process should be included in the design phase of the localisation unit as part of the OBU. Then, the designed structure can have the capability of verifying the GNSS receiver measured train location together with other sources. With this, the acceptance of possible measurement errors are also verified to see whether the error is acceptable as still accepting GNSS receiver measured train location to be on the track.

From the GNSS receiver side, there has been integrating **R**eceiver **A**utonomous **I**ntegrity **M**onitoring (RAIM) or the newly developed NIORAIM [74] algorithms to observe the integrity of the GNSS receivers. When there are more than four pseudoranges used for determining the GNSS receiver location, a least square residual can be calculated from the final measurement result and the pseudoranges, this residual is often used as a measure of the quality [75], and is normally called RAIM. RAIM algorithm uses only the "snapshot" of measurement pseudorange, there area many derived algorithms from this, including pseudorange comparison method [76], the least square residual method [77], parity space method [78]. From the mathematical point of view, they equal to each other [79]. In most GNSS receivers, normally the least square residual method and parity method is widely used. The earlier paper on RAIM techniques dates back to the one presented by Bradford W. Parkinson and Penina Axelrad in 1988 [77]. After that, there are many improvements for the similar algorithms. Researchers are also trying to apply similar algorithms into railway applications. For example, a sequential RAIM was proposed by Igor V. Nikiforov to improve GNSS for safe rail operations [80].

For the composition of a verifiable localisation unit, Karl-Albrecht Klinge and other colleagues from iVA TU Braunschweig designed a localisation unit with inertial sensor, GNSS receiver, and GNSS reference receiver (for differential GNSS) together to deliver failure tolerable location of the vehicle [81]. This structure uses the GNSS receiver location with a failure model to provide correction data for the inertial sensor.

From the localisation unit perspective, χ^2 testing is widely used for fault diagnose. The good side is no state equation is needed, the measurement directly reflects the performance of each GNSS receiver measured train location. Adrian Waegli analysed the coupled localisation unit of GNSS/**I**nertial **M**easurement **U**nit (IMU) together. He proposed a integrated IMU sensor fusion structure, then analysed the geometry of satellites. This method is good for detecting the error and no error propagation will affect the following measurements [82].

For railway applications, Jiang Liu proposed a localisation unit structure of GNSS, odometer, and **I**nertial **N**avigation **S**ensor (INS) together, the system has a principle component analysis fault detection method, and also a probability based filter for GNSS receiver measured train location verification [83].

Jana Heckenbergerova from Czech Republic proposed a discrete train location integrity monitoring algorithm to monitor the GNSS measurements along with the digital track map to verify the GNSS receiver measured train location deviation and thus calculate the horizontal protection limit [84].

The application of the methodology or algorithm are applicable for the GNSS-based localisation unit. The ultimate goal is to use the GNSS receiver measured location and quickly verifying the train locations measured by the GNSS receiver. In this dissertation, the verification procedure is achieved through two steps. The first step is the comparison of GNSS receiver measured train location with the digital track map, the second step is the comparison of the accepted train location together with the relative mileage estimated from both the Doppler radar velocity and GNSS receiver velocity in the given time interval.

Chapter 3

Fundamentals of Used Means of Descriptions and Theories

This chapter introduces the methodologies as the basis for the objectives introduced in Chapter 1: terminology migration, evaluation, and verification. The methodologies are UML class diagram and attribute hierarchy for terminology migration methodology, Petri net and statistics for evaluation methodology, and optimal detection theory for verification methodology.

3.1 UML Class Diagram

This section introduces the UML used in this dissertation as one means of description for introducing the structure of both systems and concepts.

UML is a graphical language that may be used to visualise, specify, construct, and document the artifacts of a software-intensive system [85]. The UML is appropriate for modelling software as well as workflow, structure, and behaviour of a system. UML can also be used for designing the hardware. Basically, UML is only a modelling language.

The vocabulary of the UML encompasses three kinds of building blocks: things, relationships and diagrams. Things are the abstractions; relationships tie these things together; diagrams group interesting collections of things. This dissertation uses UML class diagram as the diagram for modelling. The related building blocks are introduced as follows.

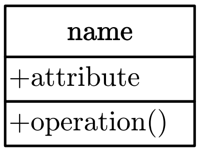


FIGURE 3.1: Class as a Kind of Structure Things for UML Class Diagram

3.1.1 Class

Class is one of the structural things of the UML class diagram. Structural things are the nouns of UML models. They are mostly static parts of a model, representing elements that are either conceptual or physical. Class is used in this dissertation as one kind of structural things.

Definition 3.1 Class (from [85])
Class is a description of a set of objects that share the same attributes, operations, relationships, and semantics. A class implements one or more interfaces. Graphically, a class is rendered as a rectangle, usually including its name, attributes, and operations.

Remark 3.1 Class Graphical Representation
The class notation permits to visualise graphically an abstraction apart from any programing language and in a way to emphasise the most important parts of an abstract: its name, attributes, and operation. A class example in Figure 3.1 shows the structure of a class. The + sign besides the attribute and operation mean that both attribute and operation are public. Besides, the attribute as system property is deeply used in Section 3.2.1 Chapter 3. Operations are not concerned in this dissertation. In some situations in the dissertation, classes are illustrated as a simple box such as in Figure 3.3.

Besides classes, the structural things also contain interfaces, collaborations, use cases, and so on. Since they are not used in this dissertation, the definitions are not introduced.

3.1.2 Relationships

There are many kinds of relationships in UML class diagram, only two of them are used in the dissertation, they are generalisation and association. For association, more sophisticated relations are also used in the dissertation: multiplicity, aggregation and composition.

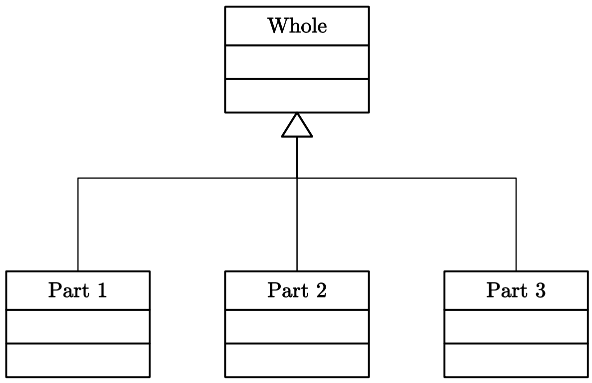


FIGURE 3.2: Generalisation as a Kind of Relationship in UML Class Diagram

Definition 3.2 Generalisation (from [85])
A generalisation is a relationship between a general class (called the "supper class" or "parent") and a more specific kind of that (called the "subclass" or "child"). Generalisation is sometimes called an "is-a-kind-of" relationship.

Remark 3.2 Generalisation Example
A class may have zero, one or more parents. A class that has no parents and one or more children is called a root class or a base class. Most often, generalisations among classes are used to show inheritance relationship. A generalisation example is shown in Figure 3.2.

Definition 3.3 Association (from [85])
An association is a structural relationship that specifies the objects of one thing are connected to objects of another thing. Graphically, an association relationship is rendered as a solid line, possibly directed, occasionally including a label, an association connects the same or different classes. An association is a more general relationship, it derives multiplicity, aggregation and also composition. These three kinds of associations represent the association between classes more in detail.

Definition 3.4 Multiplicity (from [85])
An association represents a structural relationship among classes. In many modeling situations, it's important to state how many objects may be connected across an instance of an association. This "how many" is called the multiplicity of an association's role.

Remark 3.3 Multiplicity Representation
In this dissertation, the "how many" is used as one (1) and one or more (1...$*$). An example of two multiplicity is shown in Figure 3.3. The (1) to (1) shows between class 1 and class 2 there is only one and only one association. The (1) to (1...$*$) shows class 1 may have many class 2.

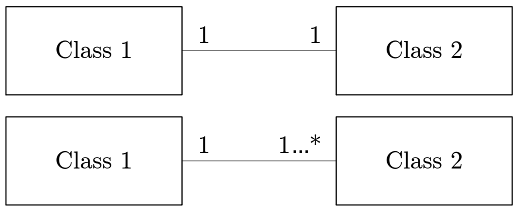


FIGURE 3.3: Multiplicity as a Kind of Relation in UML Class Diagram

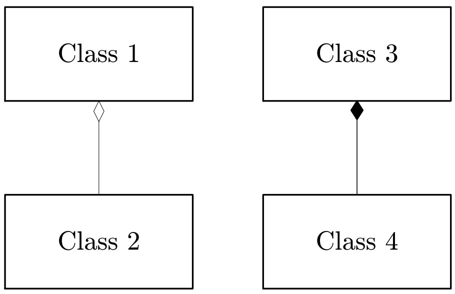


FIGURE 3.4: Aggregation (left) & Composition (right)

Definition 3.5 Aggregation (from [85])
An aggregation is a plain association between two classes representing a structural relationship between peers, meaning that both classes are conceptually at the same level, no one is more important than the other.

Definition 3.6 Composition (from [85])
Composition is a variation of simple aggregation, with strong ownership and coincident lifetime as part of the whole. Parts with non-fixed multiplicity may be created after the composite itself, but once created they live and die with it.

Remark 3.4 Difference between Aggregation and Composition
Aggregation turns out to be a simple concept with some fairly deep semantics. Simple aggregation is entirely conceptual and does nothing more than distinguish a whole from a "part". Simple aggregation does not change the meaning of navigation across the association between the whole and its parts, nor does it link the lifetime of the whole and its parts. In composite aggregation, an object may be part of only one composite at a time. Aggregation is specified by adorning a plain association with a empty diamond at the whole end, meanwhile composition is specified using a filled diamond. The example of both is shown in Figure 3.4.

3.1.3 Diagrams

Diagrams are the means by which you view these building blocks. A diagram is a graphical presentation of a set of elements, most often rendered as a connected graph of things and relationships [85]. Typically, when viewing the static parts of a system using one of the four following diagrams:

1. class diagram
2. object diagram
3. component diagram
4. deployment diagram

Class diagrams are the most common diagram found in modelling object-oriented systems and also concepts.

Definition 3.7 Class Diagram (from [85])
A class diagram shows a set of classes, interfaces, and collaborations and their relationships.

The examples for UML class diagrams has been shown in Figure 3.2, Figure 3.3, and Figure 3.4.

3.2 Consistent Terminology

The first step that needs to be done for GNSS for train localisation evaluation and verification is to find the common properties for both GNSS in space from service provider side and GNSS receiver in railway applications from the user side. The heterogeneous understanding of terms is the essential difficulty of inter-domain communication. Clearly controlled definition of terms are used to reduce ambiguity and complexity by reducing a wide range of possibilities of interpretations to an essential and common understanding subset. So terminology is treated as the basis bracket for the research of safety-related applications.

The conceptual content of a linguistic sign is constituted by the semantic relation of other linguistic signs. The concept can derive the corresponding controlled and specified research domain which can be treated as the property of the concept, going deep a model can be built. This new model of a linguistic sign is of immense explanatory power for the differences which currently exist between the same term used in different application domains and different terms for the same application domain. Using this approach it will be possible to model concepts in its complete complexity. For this reason a major focus is laid on linguistic relations such as different degrees of synonymy, homonym, overlapping terminology, equivalence, domain specificity, multiple possibilities of translation etc. This approach is leading a formalisation of the terms.

3.2.1 Attribute Hierarchy for Concept Intension

Definition 3.8 Concept
Concepts will be defined as "unit of thoughts of a group or class of objects formed by common properties, the properties determine the meaning of the abstraction" according to DIN 2342 [86]. Concepts are used to detect objects of understanding about objects and the conceptual ordering of objects. A concept has intension and extension. A term is used to name a concept.

The intension of a concept is any property or quality connoted by the concept [86]. On the opposite side, the extension of a concept consists of the things to which a term applies [86]. For example, the intension of "GNSS" defines the properties of it as *satellites* determine user *location*. The extension of "GNSS" can be GPS, Galileo, etc.

The intension of a concept is described using property, characteristic, quantity, value, and unit. This structure is called attribute hierarchy by the *iglos* research group at the Institute of Traffic Safety and Automation Engineering (iVA) [87] [88] [89] [90] [91], the attribute hierarchy is inspired and developed from Rudolf Carnap's contribution [92]. A description of this method is displayed in UML class diagram [93] in Figure 3.5. The definitions of property, characteristic, quantity, value, and unit are as follows.

Definition 3.9 Property
Properties are related to the generally and abstractly perceivable states of reality. Properties can be expressed in natural language by denominations and present terms in the sense of the previously presented meta linguistic model. For a precise terminological clarification, the observed properties are based on empirical observable characteristics. Properties develop by an abstraction of characteristics.

Definition 3.10 Characteristic
Characteristics are basic elements for the recognition and description of objects and consequently a major for the order within a terminology building. Characteristics

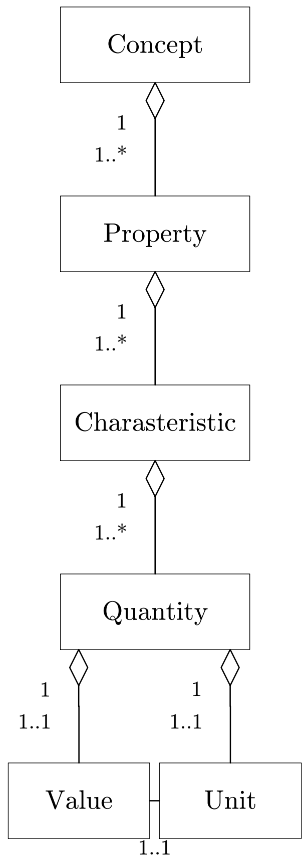


FIGURE 3.5: Attribute Hierarchy for Term Intension in UML Class Diagram

are objectively determinable and therefore in objective way of specified properties. The properties of objects of the extra linguistic reality become quantifiable or measurable by them. An object can show characteristic values of different characteristics but only one characteristic value of each characteristic corresponds to it. These characteristic values have to be determined in a sufficiently specified way for the particular purpose. Thus, there have to be a principal method (e.g. observation, proving, test, counting and measurement) for determining the characteristic properties for a given characteristic holders. This is normally the specification of a system of characteristic values (scale level) which shows how to classify the characteristic value. Characteristics are accessible for a measurement (continuous characteristics) or counting (discrete characteristics).

Definition 3.11 Quantity

Physical quantities are related to a class of classes of physical phenomena or to a class of physical properties which amount a scale of numeric indicated value and which can be ascribed to concrete phenomena which can be produced under well-defined experimental conditions. The determination of physical quantity includes in addition to the topological definition (equivalence and order relation) the metric definition (determinations in relation to scale forms, zero point and unit). A continuing distinction of quantities between basic quantities and derived quantities is the result of this embedding of a particular quantity into a quantity system.

Definition 3.12 Value
Values of a quantity can be presented as a product of numerical value and scale unit. In this context, the scale unit is a defined real scalar value by international agreement with which any other value of the quantity can be compared. As numerical value, it can be expressed as relation of both quantity values. Analogous to the quantity, it can be also differentiated between basic unit (second as basic unit of the quantity time) and derived unit in relation to units, e.g. Failure in Time (FIT) as derived unit of the quantity failure rate which is quoted in number of failures in 10^9 hours.

Definition 3.13 Unit
A unit of measurement is a definite magnitude of a physical quantity, defined and adopted by convention or by law, that is used as a standard for measurement of the same physical quantity. Any other value of the physical quantity can be expressed as a simple multiple of the unit of measurement.

The attribute hierarchy can be divided into two levels. One level is the terminology foundation, the other level is the qualitative evaluation or quantitative numbers. This is the process from the basic abstraction to a real measurement. Each concept is introduced in this structural diagram. The concepts can be interpreted from properties, there could be one or more properties, so it is shown as $(1...*)$. The other parts of this attribute hierarchy are following the same philosophy.

This kind of hierarchy sets up the identical structure for different concepts. It generates the interpretations of different concepts in the same way. So by this method, the difference between similar concepts can be easily judged and analysed. This is of great help to distinguish the different requirements of GNSS for different applications. This is shown in detail in Chapter 4, and then analysed in the migration process in Chapter 5.

3.2.2 System as a Concept in UML Class Diagram and Attribute Hierarchy

System is a very important concept. System as the basis for uniformed connotation should be defined as general as possible. The system can be interpreted by four basic principles: structure principle, decomposition principle, causal principle, and

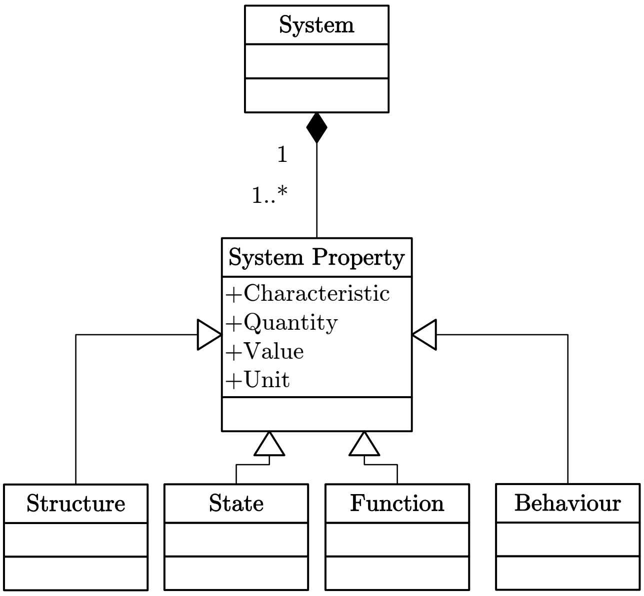


FIGURE 3.6: Elementary Properties of System Model Concept in UML Class Diagram [94]

temporal principle [94]. Among these principles, the decomposition principle is the most important for understanding the complexity and the general system properties.

The decomposition principle (in German language "Dekompositionsprinzip") shows the system is composed of components. The relation between the components build up the system structure. The components can be characterised through properties, then the properties are specified through characteristics, the characteristics are described by quantity; normally the quantity is composed by value and its unit [94] [95]. The relation can be illustrated using UML class diagram [93] in Figure 3.6. The definition of the terms in Figure 3.6 are cited from the VDI 4004 [96]. This standard defines the essential terms, this decomposition structure is used as the foundation.

The system is decomposed into four properties: structure, state, function, and behaviour. Then these four concepts are defined in the attribute hierarchy. This brings the system and the concept into the same form of definition for this dissertation.

For example, the structure of a GNSS system is composed by three segments: space segment, control segment and user segment. The state of a GNSS system can be defined as usable state, unusable state. The function of a GNSS system is to provide locations with the satellites. And, the behaviour of the system can be evaluated through evaluation methodologies about the performance of the behaviours, such as accuracy, etc.

The four concepts are further defined and compared in Chapter 4 for the three different systems investigated in this dissertation.

3.2.3 Relation between Terms

It is necessary to analyse and differentiate the relation between terms. The right relation between two terms helps to differentiate the concepts based on the terms. The terms are referring to each other. A relation always consists two terms. One of the terms performs the role of a subject, and the other performs the role of an object. The relation between two terms is specified by a relation type.

Definition 3.14 Relation Between Two Terms
Relation is an unspecified connection between terms. Relation simply indicates that there is a connection existing between two terms, but not of which sort it is. By the subordinate relation types, this relation can be further specified. If there are uncertainties concerning the type of relation between two terms, but simultaneously assurance about the existence of a relation, this may be indicated by a relation [97].

The terms in the attribute hierarchy shown in the UML class diagram are represented through the relationship types in UML. They are generalisation, association, and multiplicity. These relationship types in UML show the hierarchical relationships for terms. There are other relations need to be defined and compared for the consistency of the terminologies.

There are two level of relations. The first level are the elementary relation types, the second level are the specific relation types. The elementary relation types serve as the first relation of terms and the construction of a rough terminological structure that relates terms linguistically and conceptually. The specific relation types can be used to give a more accurate model of the terminological system, thus they are more specific relation types after elementary relation types. The relation types and the meaning of them are shown in Table 3.1.

An example showing the relation between two terms “continuity” and “reliability” is stated below. The attribute hierarchy representation of the two terms is shown in Figure 3.7. The definitions of both continuity and reliability show only difference in the names. That is to say, the “continuity” can be replaced by “reliability”. But concerning the attributes in attribute hierarchy, the failure rate of “continuity” λ_c and the failure rate of “reliability” λ_r, shows that $\lambda_r = \lambda_c + \lambda_{others}$[3]. Thus

[3]The more detailed analysis is shown in Chapter 5 Section 5.3.

TABLE 3.1: Relation Types in the Dissertation

Elementary Relation Type	Specific Relation Type	Definition
risk of confusion	mixed up with	one of the possible or commonly used translations as the preferred translation
translation	has translation	the two terms are the same meaning, but in different languages
hierarchy	has part of	same as UML composition relationship
	has equivalence definition	texts of their definitions differ only in formulations but not in their general content

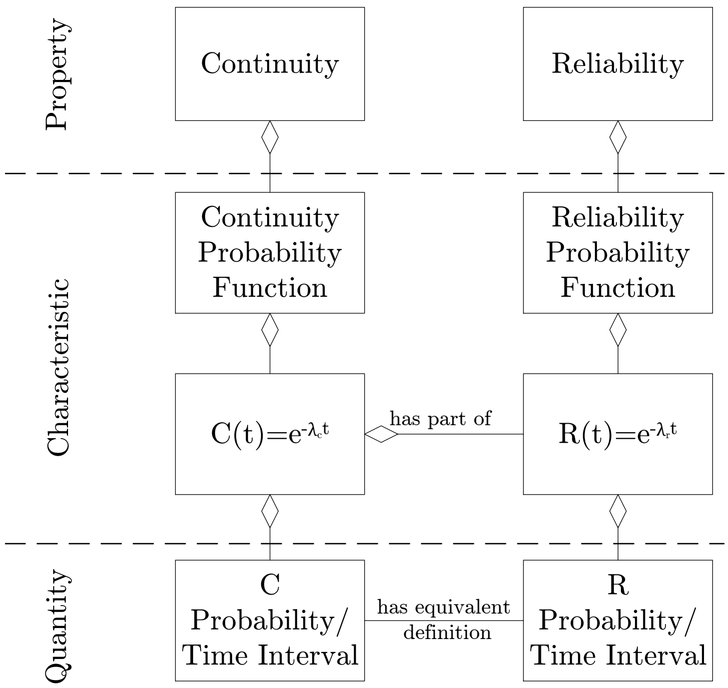


FIGURE 3.7: Relation between “Continuity” and “Reliability”

$R(t) < C(t)$, which means reliability is part of the continuity in definition and also in formulation.

With the relation between the attributes, it is easier to distinguish the difference between the two properties and also find the appropriate one in the appropriate context.

3.3 Formalisation with Petri nets

Petri nets are considered as a formal and graphical means of description for system modelling. Petri nets are introduced in the PhD dissertation of Carl Adams Petri [98] at Technische Universität Darmstadt in 1962. The original theory was developed as an approach to model and analyse communication systems. Petri nets also have very strong mathematical foundation.

Since the seminal work, many representations and extensions have been proposed for allowing more concise descriptions and for representing system features not observed on the early models. The simple Petri nets have subsequently been adopted and extended in several directions, in which timed, stochastic, high-level, object-oriented and coloured nets are a few examples of the proposed extensions.

Petri nets simulate the flow of objects, their states, their creation and their vanishing. The delay of flow is modelled explicitly by the parameters of so-called transitions which are one of the two types of nodes of a Petri net [99].

3.3.1 Place/Transition nets

The base of all Petri net models is the definition of a net.

Definition 3.15 Net Definition (from [100] [101])
A net is defined by giving a set of states (denoted by S), a set of transitions (denoted by T), and a relation for "flow" or "followed by" (denoted by F) telling which old states will be replaced by which new states. Sometimes, instead of S, the letter of P is used, coming from places.

Formally it is defined as a triple $\Sigma = (P, T, F)$ where,

- P is a set of places;
- T is a set of transitions, disjoint from P ($P \cap T = \emptyset$);
- F is a flow relation $F \subseteq (P \times T) \cup (T \times P)$ for the set of arcs.

If P and T are finite, the net Σ is said to be finite.

Place/Transition nets are in a sense of net definition in Definition 3.15 together with a definition of arc weights. Place/Transition nets are one of the most prominent and best studied class of Petri nets, and it is sometimes just called **P**etri **n**ets (PN). A marked Place/Transition net is a bipartite directed graph, usually defined as follows.

Definition 3.16 Place/Transition nets (from [102])
A Place/Transition net (also called P/T net) is defined by $\Sigma = [P, T, F, W, M_0]$ where,

- $P = \{p_1, p_2, ..., p_m\}$ is a finite set of places;
- $T = \{t_1, t_2, ..., t_n\}$ is a finite set of transitions;
- $F \subseteq (P \times T) \cup (T \times P)$ is a set of arcs (flow relation);
- $W : F \to \{0, 1, 2, 3, ...\}$ is a weight function;
- $M_0 : P \to \{0, 1, 2, 3, ...\}$ is the initial marking.

Remark 3.5 Markings
Markings is the most important element to differ a net and a Petri net. It is convenient to define markings as vector of integers, assuming a total ordering of the places. With the initial marking M_0, different transitions t_i have the priority to fire, then a new marking M' is generated. For $\forall\ p_j \in P$, if $M(p_j) = k$, it means the place p_j has k tokens.

One P/T net has the following transition firing rule. For any $t \in T$, if

$$p \in P : p \in {}^{\bullet}t \to M(p) \geqslant 1$$

It means the transition t at marking M is enabled, is written as $M[t >$. When t fires, the marking M goes to a new marking M', is written as $M[t > M'$. Generally for any $p \in P$,

$$M'(p) = \begin{cases} M(p) - 1 & if\ p \in {}^{\bullet}t - t^{\bullet} \\ M(p) + 1 & if\ p \in t^{\bullet} - {}^{\bullet}t \\ M(p) & others \end{cases}$$

Remark 3.6 Elements of a P/T net and Representations (from [102])
This class of P/T nets has two kinds of nodes, place and transition. Place (P) is represented by circles and transitions (T) is represented by bars. Figure 3.8 depicts the basic elements of a simple PN. The set of arcs F is used to denote the places connected to a transition (and vice-versa).

Place and transitions may have several interpretations. Using the concept of conditions and events, places represent conditions, and transitions represent events, such that an event may have several pre-conditions and post-conditions. For more interpretations, Table 3.2 shows other meaning for places and transitions. It is important to show that there are another way to represent P/T net elements.

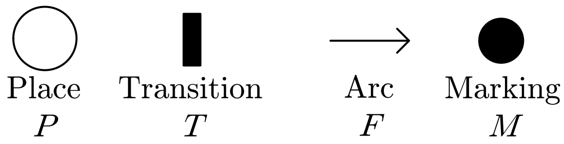


FIGURE 3.8: Petri net Basic Elements

TABLE 3.2: Interpretation for Places and Transitions

Input Places	Transitions	Output Places
pre-conditions	events	post-conditions
input data	computation step	output data
input signals	signal processing	output signals
resource needed	task performing	resource releasing
conditions	logical clauses	conclusions
buffers	processing	buffers

Definition 3.17 Reachability Graph
The state graphs, i.e. those of a momentary marking (irrespective of the details of switching delays used-up) are called reachability graphs. Since each node of the **R**eachability **G**raph (RG) of a given PN corresponds uniquely to a marking (at time τ)

$$\underline{M(\tau)} = (M_1(\tau), M_2(\tau), ..., M_m(\tau))$$

The total number of states of the RG $M(\tau)|_{\tau=1...f}$, i.e., is bounded by a finite number f when the reachability graph can be drawn.

Clearly, edges in RG correspond to the switching of transitions in the PN under discussion. Therefore the RG is a digraph with an edge marking.

3.3.2 Stochastic Petri nets

Petri nets are classic means of description for modelling and analysing discrete event systems which are too complex to be described by automata or queueing models. Time and probabilistic choices are essential aspects for a performance evaluation model. **S**tochastic **P**etri **n**ets (SPN) emerged as a modelling formalism for performance analysis in the early 1980s. SPN have two different classes of transitions: immediate transitions and timed transitions. Once enabled, immediate transitions fire in zero time. Timed transitions fire after a random, distributed enabling time [103].

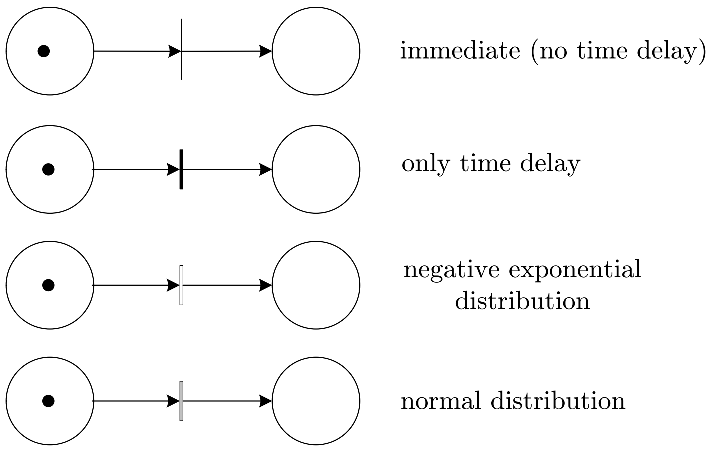


FIGURE 3.9: Stochastic Petri net Transition Category

Definition 3.18 Stochastic Petri nets (from [103])
Let $SPN = (P, T, F, W, M_0, T_1, T_2, E)$ be a stochastic Petri net, where:

- $P = \{p_1, p_2, ..., p_m\}$ is a finite set of places;
- $T = \{t_1, t_2, ..., t_n\}$ is a finite set of transitions;
- F is a flow relation $F \subseteq (P \times T) \cup (T \times P)$ for the set of arcs;
- $W : F \rightarrow \{0, 1, 2, 3, ...\}$ is a weight function;
- $M_0 : P \rightarrow \{0, 1, 2, 3, ...\}$ is initial marking;
- $T_1 \subseteq T$ is the set of timed transitions. $T_1 \neq \emptyset$;
- $T_2 \subseteq T$ denotes the rest of immediate transitions $T_1 \cap T_2 = \emptyset, T = T_1 \cup T_2$;
- $E = (e_1, ..., e_{|T|})$ is an array whose entry $e_t \in \mathbb{R}^+$.

  - e_t is a rate of negative exponential distribution/normal distribution or other distributions specifying the firing delay, when transition t_t is a timed transition, i.e. $t_t \in T_1$

  - e_t is a firing weight, when transition t_t is a immediate transition, i.e. $t_t \in T_2$

The difference between the SPN and a P/T net is only the rates on several transitions. The possible transitions appeared in this dissertation are defined in Figure 3.9.

3.4 Probability and Distribution

GNSS receivers delivers location measurements are assumed to be delivered as at a constant rate[4], the measurements can be regarded as a stochastic process. The stochastic performance needs to be studied. With the correct understanding of the measurements for this GNSS receiver, the performance characteristics can be used to detect and predict the ongoing measurement outputs from the GNSS receiver.

3.4.1 Probability

Probability is a measure or estimation of how likely it is that something will happen or that a statement is true. Probabilities are given a value between 0 (0% chance or will not happen) and 1 (100% chance or will happen). The higher the degree of probability, the more likely the event is to happen, or, in a longer series of samples, the greater the number of times such event is expected to happen.

Definition 3.19 Random Variable (from [104])
Considering a random experiment having sample space S, A is a random variable, X is a function that assigns a real value to each outcome in S. For any set of real numbers A, the probability that X will assume a value that is contained in the set A is equal to the probability that the outcome of the experiment is contained in $X^{-1}(A)$. That is:

$$P\{X \in A\} = P(X^{-1}(A)) \tag{3.1}$$

where $X^{-1}(A)$ is the event consisting of all points $s \in S$ such that $X(s) \in A$. A random variable X is said to be discrete if its set of possible values is countable.

Remark 3.7 GNSS Receiver Measurements As A Discrete Random Variable
The measurement set from the GNSS receivers is regarded as countable values not as continuous in time. So the measurement set is considered as a discrete random variable X. The following definitions, theorems as well as remarks will consider only based on discrete random variable.

Definition 3.20 Distribution of A Random Variable (from [105])
When a probability distribution has been specified on the sample space s of an experiment, we can determine a probability distribution for the possible values of any random variable X. A is any subset of the real line. Denote $P(X \in A)$ the probability that the value of X belongs to subset A. Then $P(X \in A)$ is equal to the

[4] But the GNSS receiver clock jitter problem exists in the measurements.

probability that outcomes s of the experiment will be such that $X(s) \in A$. That is:

$$P(X \in A) = P\{s : X(s) \in A\} \tag{3.2}$$

Definition 3.21 Distribution Function (from [104])
The distribution function F of the discrete random variable X is defined for any real number x by:

$$F(x) = \sum_{y \leqslant x} P\{X = y\} = P(X \leqslant x), -\infty < x < \infty \tag{3.3}$$

in that $F(x) \leqslant 1$. In reliability theory, $F(x)$ is used to describe the probability of failure for the system, at the specific time x, $F(x)$ is describing the probability the system is failed [106].

Definition 3.22 Probability Density Function (from [104])
A **P**robability **D**ensity **F**unction (PDF) is a function that describes the relative likelihood for this random variable to take on a given value. It can be derived from the distribution function $F(x)$.

$$f(x) = \frac{d}{dx} F(x) \tag{3.4}$$

Definition 3.23 Expectation (from [104])
The expectation or mean value of the discrete random variable X, denoted by $E[X]$, is defined by:

$$E[X] = \sum_{x} x P\{X = x\} \tag{3.5}$$

The mean value is named as μ, in this situation $\mu = E[X]$.

Definition 3.24 Variance (from [104])
The variance of the random variable X is defined by:

$$\begin{aligned} var(X) &= E[(X - E[X])^2] \\ &= E[X^2] - E^2[X] \end{aligned} \tag{3.6}$$

Normally, the square root of $var(X)$ is called standard deviation. In that it is represented by $\sigma = \sqrt{var(X)}$.

3.4.2 Distributions

In this dissertation, the negative exponential distribution, normal distribution, gamma function, chi-squared distribution, student t-distribution are used. This subsection introduces these distributions in detail.

Definition 3.25 Negative Exponential Distribution (from [104])
The negative exponential distribution is a family of continuous probability distributions. It describes the time between events in a Poisson process. The PDF can be defined as:

$$f(x;\lambda) = \begin{cases} \lambda e^{-\lambda x} & x \geqslant 0 \\ 0 & x < 0 \end{cases} \tag{3.7}$$

Definition 3.26 Normal Distribution (from [104])
In probability theory, the normal distribution or Gaussian distribution is a very commonly occurring continuous probability distribution - a function that tells the probability of a number in some context falling between any two real numbers. The probability density function is denoted by:

$$f(x;\mu,\sigma) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{3.8}$$

Normally a normal distribution is written as $X \sim N(\mu, \sigma)$. It is called standard normal distribution when $\mu = 0, \sigma = 1$, and is denotes as $X \sim N(0, 1)$.

Definition 3.27 Log-normal Distribution (from [107])
A Log-normal distribution is a continuous probability distribution of a random variable whose logarithm is normally distributed. If X is log-normally distributed, then $\ln X$ is normally distributed. The probability density function of Log-normal distribution is given by:

$$f(x;\mu,\sigma) = \tfrac{1}{x\sigma\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{lnx-\mu}{\sigma})^2} \quad x > 0 \tag{3.9}$$

Definition 3.28 Rayleigh Distribution (from [107])
Rayleigh distribution is often observed when the overall magnitude of a vector is related to its directional components. A random variable R is Rayleigh distributed if $R = \sqrt{X^2 + Y^2}$, where $X \sim N(0, \sigma^2)$ and $Y \sim N(0, \sigma^2)$ are independent normal random variables. The commonly used σ is the only parameter for Rayleigh distribution. The probability density function of Rayleigh distribution is given by:

$$f(x;\sigma) = \tfrac{x}{\sigma^2} e^{-\frac{x^2}{2\sigma^2}} \quad x \geqslant 0 \tag{3.10}$$

Definition 3.29 Gamma Function (from [105])
The gamma function (represented by the capital Greek letter G) is an extension of the factorial function, with its argument shifted down by 1, to real and complex numbers. That is, if n is a positive integer, then $\Gamma(n)$ is denoted by:

$$\Gamma(n) = (n-1)!$$

For positive half integers, the function values are given exactly by:

$$\Gamma(\frac{1}{2}n) = \sqrt{\pi}\frac{(n-2)!!}{2^{\frac{n-1}{2}}}$$

Definition 3.30 Chi-squared Distribution (from [105])
The chi-squared distribution (also chi-square or χ^2-distribution) with n degrees of freedom is the distribution of a sum of the squares of n independent standard normal random variables. It is one of the most widely used probability distributions in inferential statistics, e.g., in hypothesis testing or in construction of confidence intervals.

If $X_1, X_2, ..., X_n$ are independent, standard normal distribution random variables as $N(0,1)$, then the sum of their corresponding squares,

$$\chi^2 = X_1^2 + X_2^2 + ... + X_n^2$$

is distributed according to the chi-squared distribution with n degrees of freedom. It is usually denoted as $\chi^2 \sim \chi^2(n)$. The probability density function is:

$$f(x;n) = \begin{cases} \frac{x^{\frac{n}{2}-1}e^{-\frac{x}{2}}}{2^{\frac{n}{2}}\Gamma(\frac{n}{2}))} & x > 0 \\ 0 & x \leqslant 0 \end{cases} \tag{3.11}$$

In that, $\Gamma(\frac{n}{2})$ denotes Gamma function, which has the closed-form value for integer n.

Definition 3.31 Student t-distribution (from [105])
Student t-distribution or simply (t-distribution) is a family of continuous probability distributions that arises when estimating the mean of a normally distributed population in situations where the sample size is small and population standard deviation is unknown.

If X is the standard normal distribution as $X \sim N(0,1)$, Y is the chi-squared distribution as $Y \sim \chi^2(n)$, and X and Y are independent, the random variable:

$$T = \frac{X}{\sqrt{Y/n}}$$

is with n degrees of freedom. It is denoted as $T \sim t(n)$. The probability density function of t-distribution is given by:

$$f(t;n) = \frac{\Gamma(\frac{n+1}{2})}{\sqrt{\pi n}\Gamma(\frac{n}{2})}(1+\frac{t^2}{n})^{-\frac{n+1}{2}} \quad -\infty < t < +\infty \tag{3.12}$$

3.4.3 Distribution Fitting

Distribution fitting, or to be more precisely probability distribution fitting, is to fit a probability distribution to a series of measured data concerning the repeatness of a variable phenomenon. In the context of this dissertation, it is to find the accuracy distribution of GNSS receiver calculated train location measurements. Besides, the other properties of GNSS for train localisation distribution performance can also be estimated through distribution fitting.

With the fitted distribution, the fitting result can be used to predict the probability of the failure and forecast the frequency of occurrence of the magnitude of the failure in a given time interval. The selection of the appropriate distribution depends on the presence or absence of symmetry of the data set with respect to the mean value.

There are three kinds of distributions: symmetrical distribution, negatively skewed distribution (skew distribution to the left), positively skewed distribution (skew distribution to the right). The latter two kinds are non-symmetrical distributions. The distributions introduced in the last subsection are categorised into these three kinds:

- symmetrical distribution: normal distribution, student t-distribution;
- negatively skewed distribution: negative exponential distribution;
- positively skewed distribution: Log-normal distribution, Rayleigh distribution, chi-squared distribution.

The fitting techniques are parametric methods or regression methods. In this dissertation, the parametric methods are considered, mainly the maximum likelihood method is used. With the fitted distribution, the parameters can be used together with the stochastic Petri net model to estimate the GNSS performance at the system level.

3.5 Optimal Detection Theory

The GNSS measurements normally contain errors and measurement noise. In this dissertation, the errors are called deviations[5]. Normally, the deviations needs to be evaluated to see whether the deviations are too large to be used for train localisation, thus an optimal detection methodology is needed. Statistical tools enable systematic solutions for optimal detection and decision making, this provides the ability to detect the GNSS measurement deviations and optimal detection of big deviations. The most general and popular way is using hypothesis testing methods [105] [108].

3.5.1 Hypothesis Testing

The raw material of a statistical investigation is a set of observations, these are the values taken by the random variables X whose distribution $P(X)$ is at least partly unknown. The need for statistical analysis stems from the fact that the distribution of X, and hence some aspect of the situation underlying the mathematical model is not known. The consequence of such a lack of knowledge is uncertainty as to the best mode behaviour. The problem is to determine a rule which, for each set of values of the observations, specifies what decisions should be taken.

Hypothesis testing is appropriate for situations in which one wants to guess which of two possible statements about a population is correct.

Definition 3.32 Samples and Estimate
A reasonable guess of the unknown value of a designated quantity, e.g. the mean or the variance. The quantity that hoping to guess is called *estimand.*

From the mean value perspective, suppose the estimand is μ. Considering a sample $\overrightarrow{x} = \{x_1, ..., x_n\}$ in that $\mu = \overline{x_n}$ for the mean value.

$$\overline{x_n} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

A random variable that is a function of the random variables $X_1, ..., X_n$, and is represented as

$$\overline{X_n} = \frac{1}{n}\sum_{i=1}^{n} X_i$$

This is the rule for guessing, an *estimation procedure* or *estimator.*

[5]The error of the reference measurement system is not investigated in this dissertation.

Definition 3.33 Loss Function (from [105])
The foremost requirement of a good estimator δ is that it yield an estimate of θ' which is close to the actual value of θ. In other words, a good estimator is one for which it is highly probable that the error $\delta(\mathbf{X}) - \theta$ will be close to 0. For each possible value of θ and each possible estimate a, the number $L(\theta, a)$ measures the loss or cost to the statistician.
We assume the expectation $E[L(\theta, a)]$ is a minimum, this is called *loss function*.

Definition 3.34 Test of the Hypothesis (from [108])
Hypothesis testing or significance testing is a method for testing a claim or hypothesis about a parameter in a population, using data measured in a sample. In this method, we test some hypothesis by determining the likelihood that a sample statistic could have been selected, if the hypothesis regarding the population parameter were true.

Definition 3.35 Null Hypothesis and Alternative Hypothesis (from [108])
The null hypothesis (H_0) is a statement about a population parameter, such as the population mean, that is assumed to be true. The null hypothesis is a starting point. We will test whether the value stated in the null hypothesis is likely to be true.

An alternative hypothesis (H_1) is a statement that directly contradicts a null hypothesis by stating that the actual value of a population parameter is less than, greater than, or not equal to the value stated in the null hypothesis.

Definition 3.36 Level of Significance (from [109])
Level of significance (or significance level, denoted by α), refers to a criterion of judgement upon which a decision is made regarding the value stated in a null hypothesis H_0. The criterion is based on the probability of obtaining a statistic measurand in a sample if the value stated in the null hypothesis were true.

In behavioural science, the criterion or level of significance is typically set at 5%. When the probability of obtaining a sample mean is less than 5% ($\alpha = 0.05$) if the null hypothesis were true, then we reject the value stated in the null hypothesis. This 5% is also used as the criterion in this dissertation.

3.5.2 Hypothesis Testing for One Sample

One sample test is the traditional one in hypothesis testing. According to the accuracy evaluation, the deviation of GNSS measurements can be attributed as normal distribution.[6] Assume the normal distribution population $x \sim N(\mu, \sigma^2)$, $(x_1, x_2, ..., x_{n_1})$ is a sample from x. The parameters for the sample is recorded as:

$$\overline{x} = \frac{1}{n_1}\sum_{i=1}^{n_1} x_i,\ s_1^2 = \frac{1}{n_1 - 1}\sum_{i=1}^{n_1}(x_i - \overline{x})^2$$

The test statistic to be used depends largely on the information about the population, the information about the sample is basically μ or σ of it. There are three kinds of testings based on these two parameters with the consideration of the known and unknown of the parameters. They are:

- testing of μ with the basis of known σ,
- testing of μ with unknown σ,
- testing of σ.

For the first situation, when μ and σ are both known, it is called *one-independent sample z test*. It is the statistical procedure used to test hypothesis concerning the mean in a single population with a known variance. The test statistic can be given as:

$$z = \frac{\overline{x} - \mu_0}{\sigma/\sqrt{n}}$$

With the consideration of the hypothesis $H_0 : \mu = \mu_0 \leftrightarrow H_1 : \mu \neq \mu_0$ the rejection area is $\{|z| \geqslant k\}$, when H_0 is true, $\mu \sim N(0, 1)$, so for the significance level α the probability is regarded as:

$$P_{H_0}\{|\mu| \geqslant z_{\alpha/2}\} = \alpha$$

And the rejection region is:

$$C = \{|z| \geqslant z_{\alpha/2}\}$$

3.5.3 Hypothesis Testing for Two Samples

Two-sample hypothesis testing is statistical analysis designed to test if there is a difference between two means from two different populations. A two-sample hypothesis test could also be used to test if the mean number of defective parts produced using assembly line A is greater than the mean number of defective parts produced using assembly line B [108].

[6] Normal distribution is recognised as the most common used distribution for GNSS measurement deviations, but the real measurement deviation results can be fitted to other distributions.

Assume the normal distribution population $x \sim N(\mu_1, \sigma_1^2)$, $(x_1, x_2, ..., x_{n_1})$ is a sample from x. The population $y \sim N(\mu_2, \sigma_2^2)$, $(y_1, y_2, ..., y_{n_2})$ is a sample from y. And the samples from x and y are independent from each other. The parameters for the samples are recorded as:

$$\overline{x} = \frac{1}{n_1}\sum_{i=1}^{n_1} x_i,\ s_1^2 = \frac{1}{n_1 - 1}\sum_{i=1}^{n_1}(x_i - \overline{x})^2$$

$$\overline{y} = \frac{1}{n_2}\sum_{i=1}^{n_2} y_i,\ s_2^2 = \frac{1}{n_2 - 1}\sum_{i=1}^{n_2}(y_i - \overline{y})^2$$

The methodology for testing two samples can be regarded as different categories:

- σ_1 and σ_2 known, the hypothesis testing for $\mu_1 - \mu_2$,
- $\sigma_1 = \sigma_2 = \sigma$, the hypothesis testing for $\mu_1 - \mu_2$,
- both μ_1 and μ_2 unknown, the hypothesis testing for $\frac{\sigma_1}{\sigma_2}$.

Among the three categories, the unknown μ and unknown σ is used in this dissertation. The test statistic for it can be:

$$t = \frac{\bar{x} - \bar{y}}{S_w\sqrt{\frac{1}{n_1} + \frac{1}{n_2}}}$$

in that

$$s_w^2 = \frac{(n_1 - 1)s_1^2 + (n_2 - 1)s_2^2}{n_1 + n_2 - 2}$$

With the consideration of the hypothesis $H_0 : \mu_1 - \mu_2 = 0 \leftrightarrow H_1 : \mu_1 - \mu_2 \neq 0$ the rejection area is $\{|t| \geqslant k\}$, when H_0 is true, $t\ t(n_1 + n_2 - 2)$, so for the significance level α the probability is regarded as:

$$P_{H_0}\{|t| \geqslant k\} = \alpha$$

And the rejection region is:

$$C = \{|t| \geqslant t_{\alpha/2}(n_1 + n_2 - 2)\}$$

3.5.4 Quantitative Attribute for Detection Results

The states of nature having been partitioned into two hypotheses as H_0 and H_1. The decision maker or the decision algorithm needs to choose the two logically. If

TABLE 3.3: State of Nature V.S. Decision Choice

		State of Nature	
		True	False
Decision Choice	H_0	$(1-\alpha)$	type II error (β)
	H_1	type I error (α)	$(1-\beta)$

the decision choice is H_1 when in fact H_0 is true, then that is to say a type I error has been committed. If the decision choice is H_0 when in fact H_1 is true, then that is to say a type II error has been committed. In a safety-related application, the type II error is highly important to investigate. So comparing the states of nature and the decision algorithm, there are four possible outcomes as shown in Table 3.3, two of which are favourable and two of which are unfavourable.

Type I error is normally called **F**alse **A**larm (FA), and the probability is represented by P_{FA}, type II error is normally called **M**issed **D**etection (MD) and the probability is represented by P_{MD}. The false alarms are actually safe, because the measurements are acceptable but erroneously reported as too big deviation. On the other hand, the missed detections are dangerous, because they are unacceptable deviations, so the probability of the missed detections needs to be as low as possible for the safety-related applications.

For safety-related applications, the decision choice failures can be categorised as dangerous failures (type II error) and safe failures (type I error). The safe failures, whether detected or undetected, have no influence on the technical safety functions of the system. Dangerous failures in the safety function lead on the other hand to a dangerous state of the system. The detection failure probability analysed in the time interval can be expressed as failure rate. The type I error, false alarm rate is denoted by λ_S in an hour's time interval as safe failure rate, it is calculated through:

$$\lambda_S = \frac{P_{FA}}{time\ interval} \quad (hour)$$

The type II error, missed detection rate is denoted by λ_D in an hour's time interval as dangerous failure rate, it is calculated through:

$$\lambda_D = \frac{P_{MD}}{time\ interval} \quad (hour)$$

The connection between λ_S and λ_D is described by the safety-related factor S, the S factor gives the ratio between all dangerous failures and the total of all possible failures, see Equation 3.13.

$$S = \frac{\lambda_D}{\lambda_S + \lambda_D} \tag{3.13}$$

Safe and dangerous failures are furthermore divided into:

- Safe Detected Failures (SD);
- Safe Undetected Failures (SU) (type II error)[7];
- Dangerous Detected Failures (DD);
- Dangerous Undetected Failures (DU) (type II error).

The **D**iagnostic **C**overage (DC) parameter describes the relation between the failure rate for dangerous detected failures and the failure rate for dangerous failure. This parameter represents the ratios between the failure rates which can be detected by diagnostics and the failure rate for dangerous failures.

$$DC = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} \tag{3.14}$$

The failures can be shown graphically in Figure 3.10 as a UML representation [110] [111]. In the figure, the system performance contains failures, the failures are divided into safe and dangerous failures. Among the failures, the dangerous undetected failures are type II error and needs to be studied carefully.

GNSS for train localisation decision making are mainly relying on the software or to be more specific algorithms applied in the localisation unit. The performance of the detection algorithm needs to analyse considering both two types of errors and also evaluate the probability of both safe undetected and dangerous undetected failures.

So in the algorithm the type I error can be regarded as a false positive error, the same meaning as the false alarms. The probability of FA is the same as the significance level definition in Definition 3.36, according to this hypothesis testing is also called significance test. The probability of type I error is registered as α, in that:

$$\begin{aligned} P_{FA} &= P\{reject\ H_0 \mid H_0\ is\ true\} \\ &= P\left[test\ statistic\ >\ \tau \mid \theta = \theta_0\right] \\ &= \alpha \end{aligned} \tag{3.15}$$

[7]Safe undetected failures are type II errors since they are false but remain undetected as shown in Table 3.3.

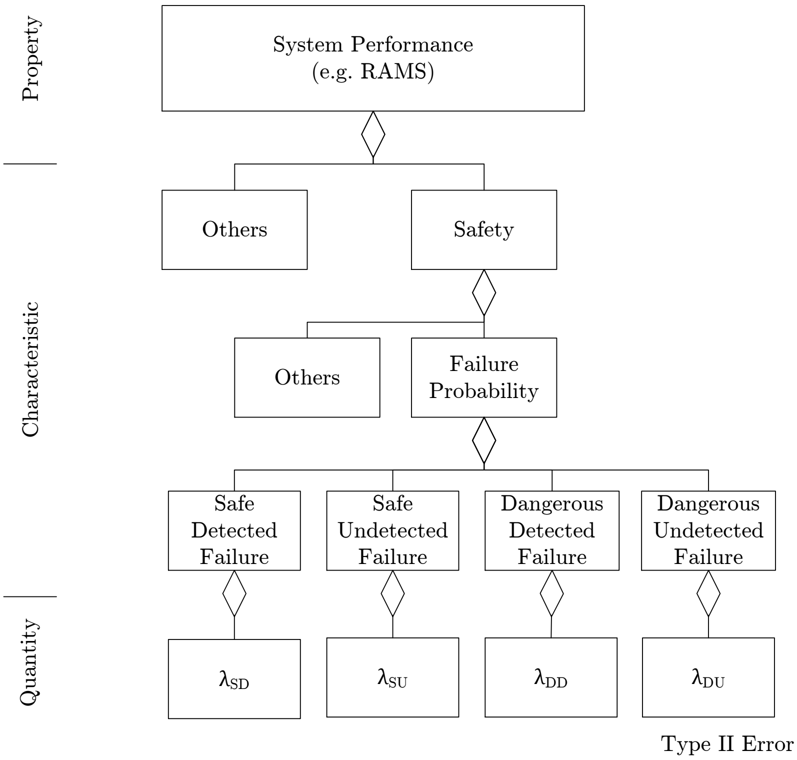


FIGURE 3.10: Failure Analysis and Rates Categories

Type II error (both λ_{SU} and λ_{DU}) is regarded as a false negative error, the same meaning as missed detections. And the probability of type II error is registered as β, in that:

$$\begin{aligned} P_{MD} &= P\{accept\ H_0 \mid H_0\ is\ false\} \\ &= P\left[test\ statistic\ <\ \tau \mid \theta = \theta_1\right] \\ &= \beta \end{aligned} \tag{3.16}$$

This two kind of failures give guidelines for the performance of the verification methodology introduced later in Chapter 7.

Chapter 4

GNSS Measurement Principles and Performance Requirements

The GNSS measurement principle is the foundation for applying GNSS into any applications. The principle is the key to the performance.

The performance requirements of GNSS are based on the idea that all applications need a minimum level of performance for the required function, and yet not all applications require the same performance requirement [112]. Thus the existing GNSS requirements for different applications also need to be studied as the reference to propose the GNSS for train localisation application.

4.1 Localisation Terminology

As one of the main work of this dissertation, it is necessary to have a clear definition and understanding of the localisation terminology. This section defines position, location and other important terms for the following parts of this dissertation. Of course, the definition starts from localisation.

Definition 4.1 Localisation
Localisation is the determination of the geographical movement state of a certain means of transportation (that means location and speed according to amount and direction in relation to a point of reference of the vehicle) in a spatial reference system [21].

Definition 4.2 Navigation
Navigation is defined as: localisation of a vehicle and its guidance from a location

Table 4.1: Positioning, Position, Localisation, and Location Definition

Terminology	Definition
positioning (DE. Positionierung)	process of putting an object in a place [21]
position (DE. Position)	the information of a place related to a coordinate system [116]
localisation (DE. Ortung)	the act of delivering a location [21]
location (DE. Ort)	location describes a position in terms of topological relations [116]

to a destination [113]. Navigation is also defined as the science of getting ships, aircraft, spacecraft or people from place to place; especially: the method of estimating location, course, and distance travelled [114].

According to the definition of location (Definition 4.1) and the definition of navigation (Definition 4.2), localisation is only part of navigation purpose. According to the current train control systems, operating a train on the railway track, the routes for the trains are already defined previously by the train time table plan and also adjusted by the train conductor at the TCC [115]. So for railway train localisation, only localisation is required.

Localisation is a process, the result of the process is a location. This process requires a resource that is the GNSS receiver. In many published documents related to GNSS, position is also used. For example GPS, in that P stands for "positioning". So "positioning" and "localisation" are mixed with each other, it is also necessary to distinguish between the two terms.

Formally, the definition of the four terms "positioning, position, localisation, location" can be treated as a data process sequence. The definition of the four terms are in Table 4.1. One thing is basically clear, the result of "positioning" is a position; and the result of "localisation" is location. Positioning and localisation distinguish from each other through resources. The resource for executing the positioning process is the energy or a person to move the object. The resource for executing the localisation process is a measurement device. So the measurement devices are trying to measure the position. But since there is always error (random error or measurement system error) inside the measurement result, the result is always called a "location".

In the context of this dissertation, the resource for "positioning" can be a train driver, the resource for "localisation" can be a GNSS receiver. The difference can

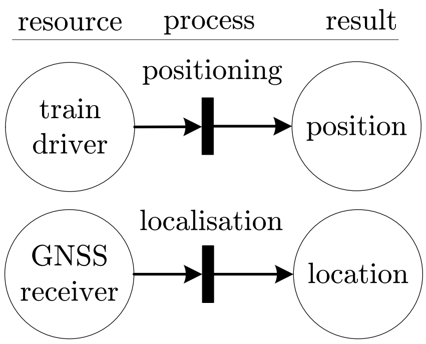


FIGURE 4.1: Positioning, Position, Localisation, Location in Petri net Interpretation

be shown clearly in the Petri net model in Figure 4.1[8]. The processes are shown in transitions, and the resources and results are shown in states.

So the train position is changing when the train is moving under the inspection of the train driver. The GNSS receiver installed on the train receives signal from the satellites, the GNSS receiver generates **GNSS receiver measured train location**. This information is transferred into a GNSS-based localisation unit, the localisation unit generates **localisation unit measured train location**. Since all the locations in this dissertation are train locations, they are simply called **GNSS receiver location** and **localisation unit location** in the following text.

But the common understood terms such as GPS, **P**ositioning, **N**avigation, and **T**iming (PNT) and so on, among them "P" actually means localisation in the definition of this dissertation. But since the abbreviations are already long time recognised by many people, the name will still stay unchanged in this dissertation[9].

4.2 Three GNSS-related Systems

The GNSS receiver location and the localisation unit location can be considered as the output of two different systems. Besides, to evaluate the GNSS receiver performance, a stand-alone reference measurement system is also built. So there are three systems applied in this dissertation, they are GNSS receiver, reference

[8]This two processes are also related, GNSS receiver is normally mounted on the train to measure the current train location.

[9]PVT is more appropriate to represent the information from a GNSS receiver. But the GNSS standards are using PNT, this dissertation follows the usage in the standards. Thus, PNT is adopted in this dissertation.

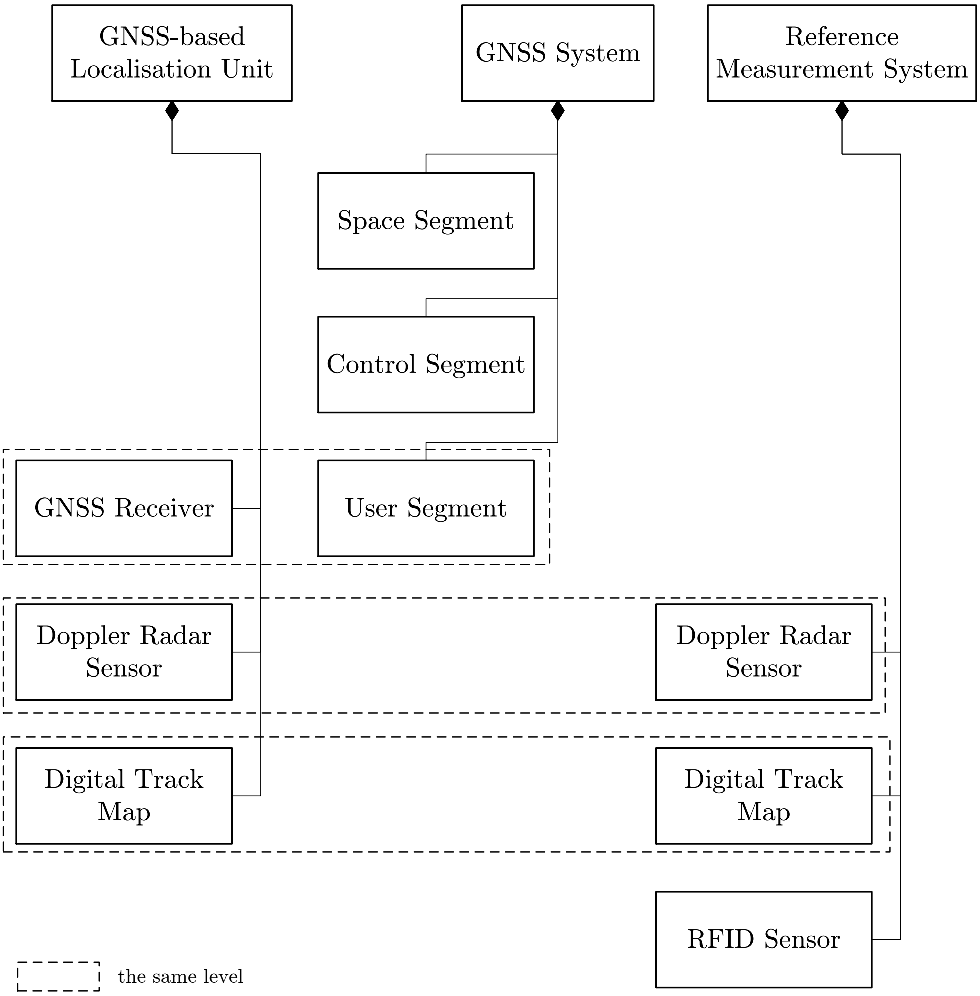


FIGURE 4.2: Three GNSS-related Systems

measurement system, and a GNSS-based localisation unit. This section is going to introduce the three systems.

The properties of the systems have been introduced in Chapter 3 Section 3.2.2 as structure, state, function, and behaviour. This section introduces the structure of each system and then illustrates the function of the GNSS-based localisation unit.

The three systems are related to each other, the relation between the three systems are shown in Figure 4.2. Basically, the GNSS-based localisation unit and the reference measurement system are both on the user segment, both need the support of a accurate digital track map.

4.2.1 GNSS Structure

The four GNSS as GPS, GLONASS, Galileo, and Beidou are sharing the same system structure. The four GNSS are comprised of three segments:

- space segment: satellite constellation;
- control segment: ground control/monitoring network;
- user segment: user receiving equipment.

All these three segments operate together to provide accurate three-dimensional PNT services to users. The following content is introducing the three segments in detail using the most mature GPS.

The satellite constellation is the set of satellites in orbit that provide the ranging signals and data messages to the user equipment. The GPS satellite constellation has 24 satellites in six 55° orbital planes, with four satellites in each plane, with room for spares. For example, currently there are 31 satellites in the sky, this number of satellites keep the availability of the satellites providing localisation service. The orbit period of each satellite is approximately 12 hours at an altitude of 20180 km [117]. With this satellite constellation, the user equipment is expected to have at least 6 satellites in view from any point of the earth. GLONASS, Beidou and Galileo use satellites in different orbits and orbit period.

The control segment (CS) tracks and maintains the satellites in space. The CS monitors satellite health and signal integrity and maintains the orbital configuration of the satellites. Furthermore, the CS updates the satellite clock corrections and ephemeris as well as numerous other parameters essential to deliver PNT services to users. The GPS control segment consists of a master control station, five base stations and three data up-loading stations in locations around the world. The base stations track and monitor the satellites via their broadcast signals. These signals are passed to the master control station where orbital parameters and timing corrections are computed. The resulting corrections are transmitted back to the satellites via the data up-loading stations.

Finally, the user receiver equipment performs the localisation, timing, or other related functions (e.g., surveying). User receiver equipments are capable of simultaneously processing the signals from a minimum of four satellites to obtain accurate location, velocity and timing measurements. However the accuracy and the reliability of the measurement is enhanced as the geometry of the satellites in good situation.

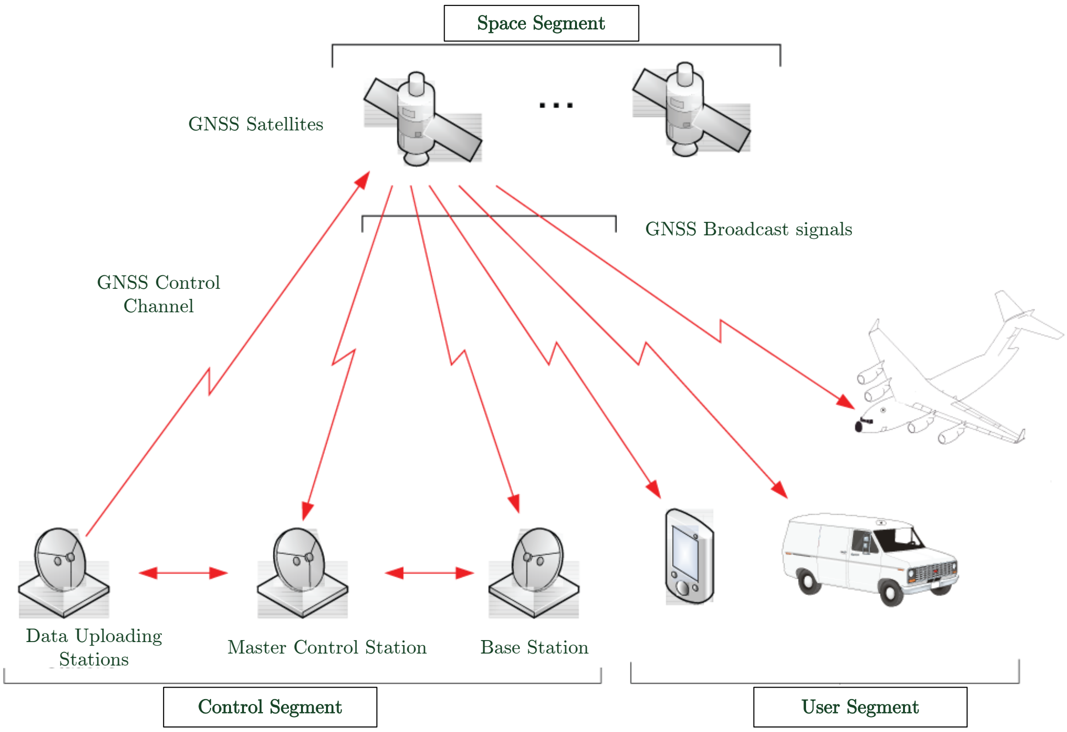


FIGURE 4.3: GNSS Segments [118]

The structure of the three segments are more vividly shown in Figure 4.3 [118]. The space segment and control segment are communicating with each other bi-directionally. But the user segment only receives signal from the satellites.

4.2.2 Digital Track Map

The digital track map is another essential component for GNSS user segment applications. This, in the content of this dissertation, means to merge the GNSS receiver measurement to the railway long-history-used mileage. The GNSS receiver measurements are always located in the 3D **W**orld **G**eodetic **S**ystem (WGS) 84 coordinate (longitude, latitude, altitude), in order to fit the measurements to mileage, an accurate digital track map is needed both for coordinate conversion and accurate localisation.

The making of a digital track map includes two processes: one is the survey of the track, the other is the database for the surveyed information. In GNSS for survey applications, more accurate GNSS receivers and techniques are requested, such as differential GNSS, **R**eal **T**ime **K**inematic (RTK) and so on. The data process of

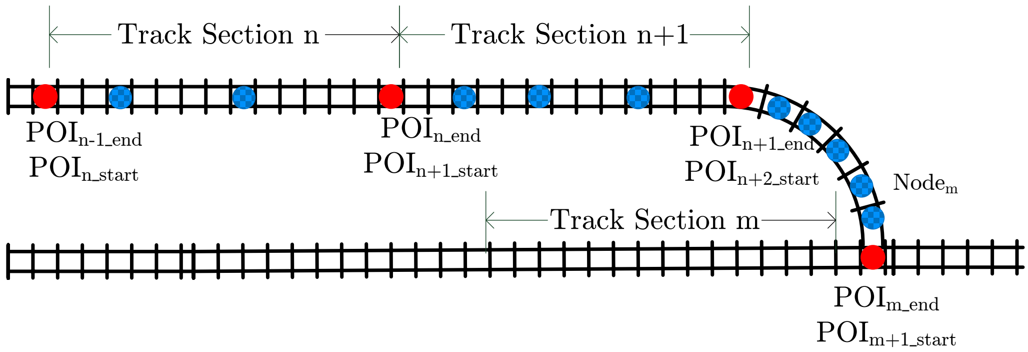


FIGURE 4.4: Structure of the Digital Track Map

the surveyed data is the other important process for making the digital track map, the process to identify the false surveyed data and exclude them is on high demand. There have been some researches on this topic for railway application scenarios [31]. The digital track map can be stored or edited using either KML [119] or XML [120] format. The XML digital track map is used in this dissertation.

The structure of the digital track map can be shown in Figure 4.4. Basically the structure of the digital track map are divided into different sections. Each section is composed by surveyed points, there are two kind of points: **P**oint **o**f **I**nterest (POI) and nodes. Each section has two POIs and a handful of nodes. The length of the section is also stored for checking the correct mileage of the train.

The structure of the XML-based digital track map can be shown as the code below. Each track is divided into many track sections, named as "tracksection" in the XML file. Then each track section is divided into many small sections, named as "section". Each small section is composed by existing measured POIs and nodes, named as "POI" and "NODE" accordingly.

```
<?xml version="1.0" encoding="utf-8"?>
<track>
        <tracksection ID = "1" Trackdistance = "32.52">
                ...
                <section ID = "n" sectiondistance = "12.42">
                        <POI ID = "POIm" WGS84_Lat = "" WGS84_Long = ""
    WGS84_Height = "" GK_East = "" GK_North = ""/>
                                <NODE ID = "NODEi" WGS84_Lat = "" WGS84_Long = ""
    WGS84_Height = "" GK_East = "" GK_North = ""/>
                                <NODE ID = "NODEi+1" WGS84_Lat = "" WGS84_Long = ""
     WGS84_Height = "" GK_East = "" GK_North = ""/>
                                <NODE ID = "NODEi+2" WGS84_Lat = "" WGS84_Long = ""
     WGS84_Height = "" GK_East = "" GK_North = ""/>
```

```
                                ...
                        <POI ID = "POIm+1" WGS84_Lat = "" WGS84_Long = ""
    WGS84_Height = "" GK_East = "" GK_North = ""/>
                </section>
                ...
                <section ID = "n+1" sectiondistance = "20.10">
                        <POI ID = "POIm+2" WGS84_Lat = "" WGS84_Long = ""
    WGS84_Height = "" GK_East = "" GK_North = ""/>
                                <NODE ID = "NODEm" WGS84_Lat = "" WGS84_Long = ""
    WGS84_Height = "" GK_East = "" GK_North = ""/>
                                ...
                        <POI ID = "POIm+3" WGS84_Lat = "" WGS84_Long = ""
    WGS84_Height = "" GK_East = "" GK_North = ""/>
                </section>
        </tracksection>
        ...
</track>
```

The XML-based digital track map is not only used for GNSS receiver performance evaluation in Chapter 6, but also applied as the basic element for GNSS-based localisation unit real-time operation verification process for matching the GNSS receiver measured train location to the track in Chapter 7.

4.2.3 Reference Measurement System Structure

A reference measurement system is a kind of localisation system, thus a subset of navigation system. The sensors, as the components of the localisation system, can be divided as active sensors and passive sensors [121]. The reference measurement system contains both active sensors and passive sensors.

In railway the alternative location measurement or detection sensors are balise [29] or odometer [122] etc. As described in the functional requirement of balise, balises are installed along the railway track as track-side equipments. They can provide 1 Hz location data only when large amount of balise group is installed along the track. This requires a lot of capital for the reference measurement system. An alternative choice is the RFID transponder installed on the track, and the RFID sensor installed on the train. In order to build a reference measurement system delivering the same frequency as GNSS receiver location, other sensors such as radar or odometer are needed. They are active sensors.

The possible structure for the reference measurement system is shown in Figure 4.5. There are three kinds of sensors forming the sensor fusion scheme: track side sensor, train side sensor, and the frozen sensor. The frozen sensor is the digital track map, which provides track information only on demand, that is a passive sensor. After a

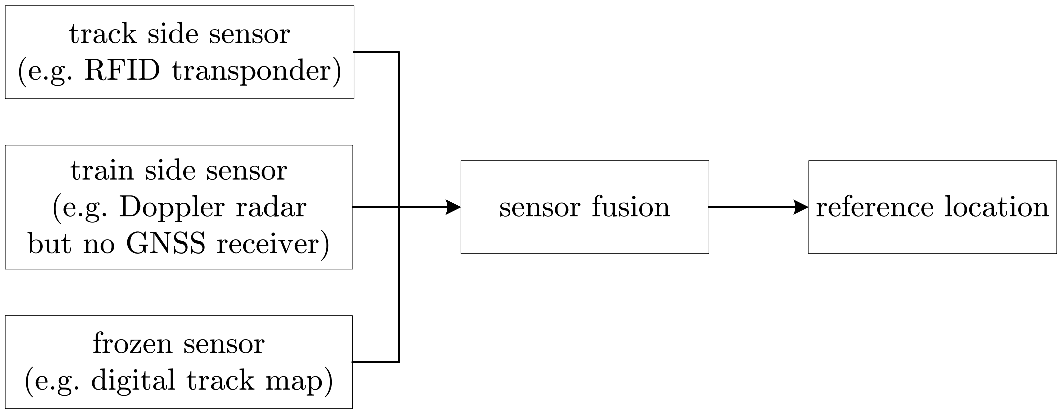


FIGURE 4.5: Structure of a Reference Measurement System

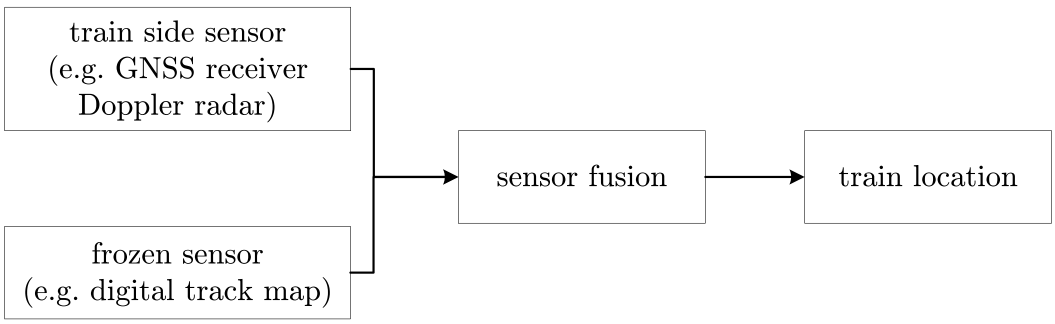


FIGURE 4.6: Structure of a GNSS-based Localisation Unit

performance evaluation of the reference measurement system, the accuracy level of the system meets the setup as "reference" of GNSS receiver location [50] [123].

4.2.4 GNSS-based Localisation Unit Structure and Functions

The structure of the GNSS-based localisation unit is shown in Figure 4.6[10]. Considering the structure of the GNSS-based localisation unit, the instances for the train side sensors can be interchanged to other localisation sensors compared in Chapter 2 Table 2.1.

Besides, the evaluation performance as the behaviour of the system is related to the functions of it. The functions of the localisation unit can be summarised in Table 4.2.

[10]The sensor fusion process means multiple resource voting structure.

Table 4.2: GNSS-based Train Localisation Unit Functions

No.	Function Descriptions
F1	receive GNSS receiver location and velocity information from GNSS receiver
F2	generate localisation unit measured train location
F3	provide the information of the location data integrity
F4	provide the information of the train driving direction

For function 1 (F1), the ability to receive GNSS receiver location, velocity and time in the required time limit is considered as highly safety-related, redundant components are on demand. The safety aspect of this function is based on the indication of information not received in time.

Function 2 (F2) is regarded as the ability of processing the received location and velocity information from GNSS receiver and processing the data with the other parts in the localisation unit such as the digital track map. The safety aspect of this function is based on the successful indication of GNSS localisation deviation under required value.

Function 3 (F3) is the self-diagnosis of the localisation unit, the integrity information also tells whether the data can be trusted or not. The safety aspect of this function is based on the correct diagnostic of the GNSS receiver location data.

Function (F4) is the driving direction information of the train. The safety aspect of this function is based on the GNSS information being accurately one after another as the time sequence and successfully matched the map.

Among the stated four functions, the F1 and F2 will be the main functions to be investigated in this dissertation.

4.3 GNSS Localisation Principles

The GNSS localisation principles is important to understand the performance of GNSS. The GNSS localisation measurement is using the time of arrival, the accuracy of the location is determined by the accuracy of time measurement.

4.3.1 Concept of Ranging Using Time of Arrival Measurements

GPS utilises the concept of **T**ime **o**f **A**rrival (TOA) ranging to determine user location. This concept entails measuring the time it takes for a signal transmitted

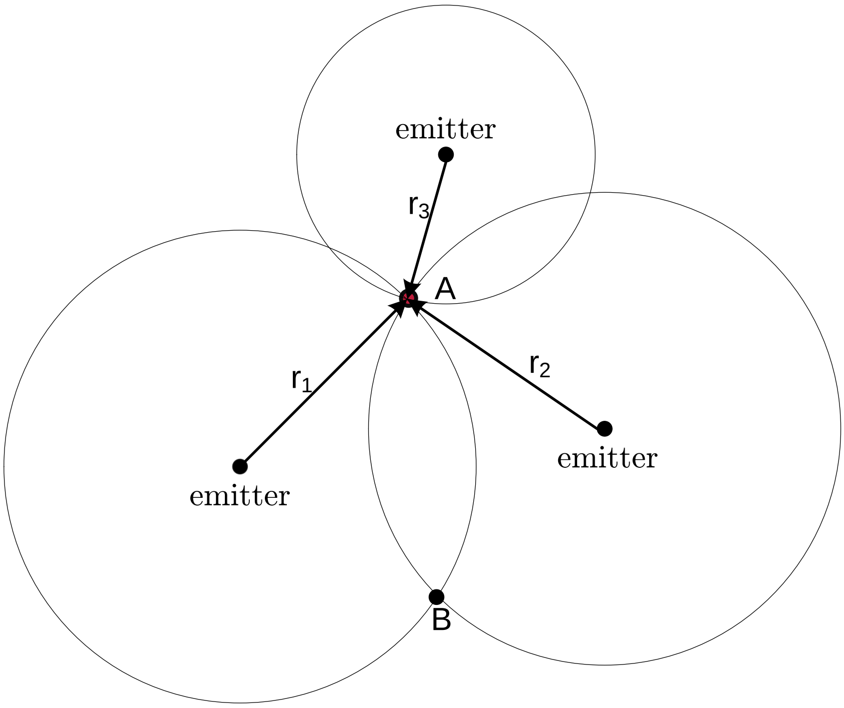


FIGURE 4.7: 2D Localisation [124]

by an emitter (e.g., foghorn, radio beacon, or satellite) at a known location to reach a user receiver.

This time interval, referred to as the signal propagation time, is then multiplied by the speed of the signal (e.g., speed of sound or speed of light) to obtain the emitter-to-receiver distance. By measuring the propagation time of the signal broadcast from multiple emitters (i.e., navigation aids) at known locations, the receiver can determine its own location. An example of two-dimensional localisation is provided in Figure 4.7.

As shown in Figure 4.7, when only two emitters are used, the user can either at place A or at place B. When there are three emitters, we can eliminate the one possibility, and determine the right place for the user. For 3D localisation, it is almost the same. Also three satellites are needed for localisation [125].

Three satellites are in some situation still enough for localisation purpose. Assuming that the user position to be measured is bounded on the earth's surface, the fourth satellite can be at the geocentric; the distance to the "fourth satellite" is the radius of the earth. Therefore the necessary fourth satellite necessary for the calculation

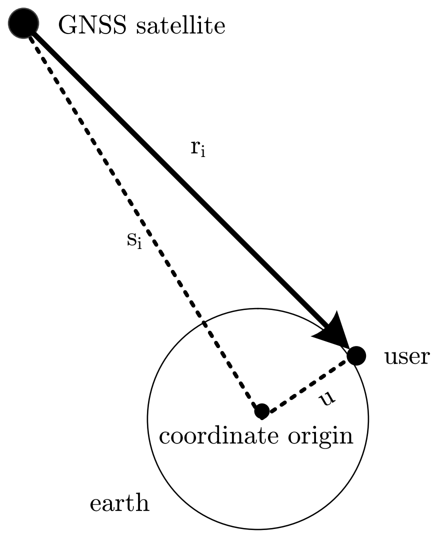


FIGURE 4.8: User and GNSS Satellite Vector Representation [124]

is given, but the calculation is restricted to the user positions on the earth surface, and the clock on the user side should be as accurate as the clock on the satellites.[11]

Generally, a signal starts from the satellite to travelling to the user from the satellite at time t_1, the user receives the signal at time t_2. Then $\Delta t = t_2 - t_1$. To calculate Δt, it needs the receiver clock and the satellite clock to be perfectly synchronised. However, the satellite and receiver clocks are generally not synchronised. The satellites have atomic clocks which can be synchronised to the level of nanosecond, but this is not the case with current receivers, as the atomic clocks are big in size and also expensive (i.e., more than \$100,000 each) [126]. Therefore, receivers manufactures use inexpensive crystal clocks. However, one nanosecond synchronisation error leads to a location error of 0.3 meters. The receiver clock will generally have a bias error from system time. Thus, a real fourth satellite is necessary to mitigate the time synchronisation error. And the range determined by the correlation process is denoted as the pseudorange ρ. To know the geometric satellite-to-user range, the following measurement and offsets need to be considered:

- the geometric satellite-to-user range r_i;
- an offset attributed to the difference between system time and the user clock $(c \times \delta t_u)$;
- an offset between system time and the satellite clock $(c \times \delta t_s)$.

[11]This is just an assumption, the clock in the GNSS receiver is far less accurate than an atomic clock.

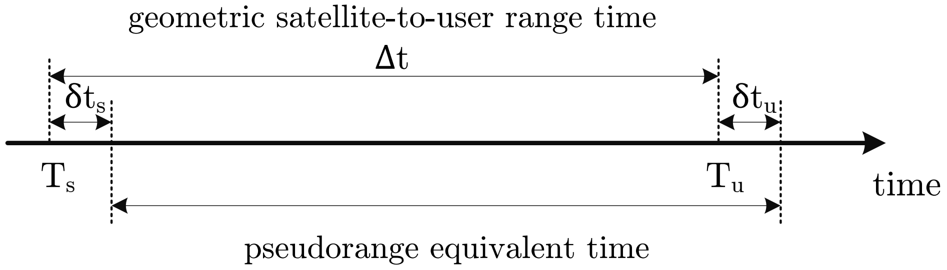


FIGURE 4.9: Range Measurement and Related Time [124]

Figure 4.8 shows the earth centre, user position, and satellite position in a relation with the vectors. In that, the vector u needs to be determined, which represents the user receiver's position in accordance with a **E**arth **C**entred **E**arth **F**ixed (ECEF) coordinate system. Set the coordinate origin of the ECEF to be $(0, 0, 0)$, the user position is (x_u, y_u, z_u). The vector s_i represents the position of the satellite i relative to the coordinate origin. So the satellite-to-user vector geometric range r_i is:

$$r_i = s_i - u = c \times \Delta t$$

As seen in Figure 4.9, the pseudorange is calculated as:

$$\rho_i = r_i + c \times (\delta t_{u_i} - \delta t_{s_i})$$

Normally the GNSS ground-monitoring network determines the corrections for these offset contributions and transmits the corrections to the satellites for rebroadcast to the users in the navigation message. Therefore, the δt_{s_i} is known by the user receiver through navigation message. Hence, the pseudorange equation can be rewritten as:

$$\rho_i - c \times \delta t_u = |s_i - u|$$

In that, the δt_{u_i} no longer related to the number i satellite, since it is affected by the user side, so it is written as δt_u in the last equation, and will be used in the following equations. With this, the equations to solve the user position is denoted by:

$$\rho_i = \sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2} + c \times \delta t_u \tag{4.1}$$

So, there are four unknown parameters (x_u, y_u, z_u and δt_u), thus at least four equations is required to calculate the parameters, a fourth satellite signal is needed. As a matter of fact, using more satellites not only allows δt_u calculation, but also increase the accuracy of user location calculation, because δt_u also contains propagation time delay etc. (measurement errors are analysed in the next part of this chapter).

So according to Equation 4.1, in order to calculate user location in a linearised measurement equation, the user position and the time offset at the user side can be considered as an appropriate component and an incremental component. The incremental component is calculated in least square and is expressed as $\Delta\rho$ as:

$$\Delta\rho = H\Delta\widehat{x} + \varepsilon \tag{4.2}$$

where $\Delta\rho$ is the misclosure vector, that is, the difference between the predicted and measured pseudorange measurements, the matrix H is the geometry or design matrix, and ε is the vector containing pseudorange measurement errors assumed to be normally distributed with zero-mean, that is $\varepsilon_i \sim N(0, \sigma_i^2)$. The epoch-by-epoch least squares localisation was used in this research instead of more practical filtering due to sensitivity analysis purposes. The incremental component from the linearisation point $\Delta\widehat{x}$ can be estimated as follows using the least square estimation:

$$\Delta\widehat{x} = (H^T H)^{-1} H^T (\Delta\rho - \varepsilon) \tag{4.3}$$

In that, the $\Delta\widehat{x}$ is denoted by:

$$\Delta\widehat{x} = \begin{bmatrix} \Delta x_u \\ \Delta y_u \\ \Delta z_u \\ -c \times \delta t_u \end{bmatrix}$$

4.3.2 Measurement Errors and Satellite Geometry

Loosely speaking, measurement error in GNSS solution is estimated by the formula

$$(error\ in\ GNSS\ solution) = (geometry\ factor) \times (pseudorange\ error\ factor)$$

Geometry factor is always regarded as DOP, and measurement errors are caused by many sources. In the last section, the range measurement uses four equations to solve δt_u, but the error still exists. The possible sources of pseudorange error are [124]:

- satellite clock error;

TABLE 4.3: GPS Standard Localisation Service Typical UERE Budget

Segment Source	Error Source	1 σ Error (m)
space/control	broadcast clock	1.1
	L1 P(Y)-L1 C/A group delay	0.3
	broadcast ephemeris	0.8
user	ionospheric delay	7.0*
	tropospheric delay	0.2
	receiver noise and resolution	0.1
	multipath	0.2
system UERE	total (RSS)	7.1*

**Note that residual ionospheric errors tend to be highly correlated among satellites resulting in location errors being far less than predicted using DOP $\times$ UERE.* [124]

- ephemeris error;
- relativistic effect;
- atmospheric effects (ionospheric, tropospheric);
- receiver noise and resolution;
- receiver dynamics and jitter;
- multipath and shadowing effects;
- hardware bias errors.

Based on the error sources, a pseudorange error budgets can be developed to show the stand-alone GNSS accuracy. The total **U**ser **E**quivalent **R**ange **E**rror (UERE) comprises components from each system segment. Table 4.3 shows the UERE budget for a single-frequency C/A code GPS receiver from both signal in space and user side [124].

The other side for measurement error is geometry which has been stated in the content before many times as DOP. Consider the 2D localisation in Figure 4.7, in the presence of accurate time synchronisation, the user location is determined by the intersection of three circles. But in the presence of measurement errors, the range rings used to compute the position will be in error thus resulting a interval for the location. Different geometry will cause different size of the intervals. This is the basic concept for DOP.

A formal derivation of the DOP relations in GPS begins with the linearisation of the pseudorange equation in Equation 4.2. The vector Δx has four components. The first three are the position offset of the user from the linearisation point; the fourth is the offset of the user time bias from the bias assumed in the linearisation point. H is the $n \times 4$ matrix:

$$H = \begin{bmatrix} a_{x1} & a_{y1} & a_{z1} & 1 \\ a_{x2} & a_{y2} & a_{z2} & 1 \\ \vdots & \vdots & \vdots & \\ a_{xn} & a_{yn} & a_{zn} & 1 \end{bmatrix} \tag{4.4}$$

In that, the $a_i = (a_{xi}, a_{yi}, a_{zi})$ are the unit vectors pointing from the linearisation point to the position of the i-th satellite. Now consider the Equation 4.3, it gives the functional relation between the errors in the pseudorange values and the induced errors in the computed location and time bias. On the assumptions, the covariance of the errors in the computed location and time bias is just a scalar multiple of the matrix $(H^T H)^{-1}$ in Equation 4.3. The covariance of dx has four components, which represents the error in the computed value for the vector of error-free position x_T. So, x_T is represented as $x_T = (x_u, y_u, z_u, c \times \delta t_u)$. The covariance of dx is a 4×4 matrix and has an expanded representation:

$$cov(dx) = \begin{bmatrix} \sigma_{x_u}^2 & \sigma_{x_u y_u}^2 & \sigma_{x_u z_u}^2 & \sigma_{x_u c\delta t_u}^2 \\ \sigma_{x_u y_u}^2 & \sigma_{y_u}^2 & \sigma_{y_u z_u}^2 & \sigma_{y_u c\delta t_u}^2 \\ \sigma_{x_u z_u}^2 & \sigma_{y_u z_u}^2 & \sigma_{z_u}^2 & \sigma_{z_u c\delta t_u}^2 \\ \sigma_{x_u c\delta t_u}^2 & \sigma_{y_u c\delta t_u}^2 & \sigma_{z_u c\delta t_u}^2 & \sigma_{c\delta t_u}^2 \end{bmatrix} \tag{4.5}$$

For easier representation of the following content, denote the relation between $cov(dx)$ and σ_{UERE} as:

$$\left\{ \frac{cov(dx)}{\sigma_{UERE}} \right\}^2 = \begin{bmatrix} D_{11} & D_{12} & D_{13} & D_{14} \\ D_{21} & D_{22} & D_{23} & D_{24} \\ D_{31} & D_{32} & D_{33} & D_{34} \\ D_{41} & D_{42} & D_{43} & D_{44} \end{bmatrix} \tag{4.6}$$

Based on Equation 4.5 and Equation 4.6, the most general parameter is termed **G**eometric **D**ilution **o**f **P**recision (GDOP) and is defined as:

$$\begin{aligned} GDOP &= \frac{\sqrt{\sigma_{x_u}^2+\sigma_{y_u}^2+\sigma_{z_u}^2+\sigma_{c\delta t_u}^2}}{\sigma_{UERE}} \\ &= \sqrt{D_{11}+D_{22}+D_{33}+D_{44}} \end{aligned} \tag{4.7}$$

So, GDOP is seen to be a function solely of the satellite/user geometry. Several other DOP parameters in common use are also useful to characterise the accuracy of the various component of the location/time solution. These are termed as **P**osition **D**ilution **o**f **P**recision (PDOP), **H**orizontal **D**ilution **o**f **P**recision (HDOP), **V**ertical **D**ilution **o**f **P**recision (VDOP), **T**ime **D**ilution **o**f **P**recision (TDOP), these DOP parameters are defined in terms of satellite UERE and elements of the covariance matrix in Equation 4.6 [127]. In this dissertation, other than general GDOP, the HDOP is used more effectively since the GNSS for train localisation is barely an horizontal localisation on the WGS84 coordinate ellipsoid. It is defined as:

$$\begin{aligned} HDOP &= \frac{\sqrt{\sigma_{x_u}^2+\sigma_{y_u}^2}}{\sigma_{UERE}} \\ &= \sqrt{D_{11}+D_{22}} \end{aligned} \tag{4.8}$$

The DOP information is transmitted to the user through NMEA data. To mention NMEA, it means NMEA 0183 in this dissertation. It is a combined electrical and data specification for communication between marine electronic devices such as echo sounder, sonars, anemometer, gyro, compass, autopilot, GNSS receivers and many other types of instruments [128]. In the GPS NMEA format, the GPGGA message contains only HDOP information, this message is used in this dissertation.

4.3.3 Environmental Scenarios in GNSS for Train Localisation

The UERE budget shows the error source from the user segment. From the user side, different environmental scenario brings no signal, shadowing, multipath, as well as other effects of the signal propagation to the accuracy degradation of the location.

In railway, the environmental scenarios along the railway track are shown in Figure 4.10. The train leaves the railway stations, going into an area with many trees. That will have signal interruption or shadowing effect. Then, the train goes into the

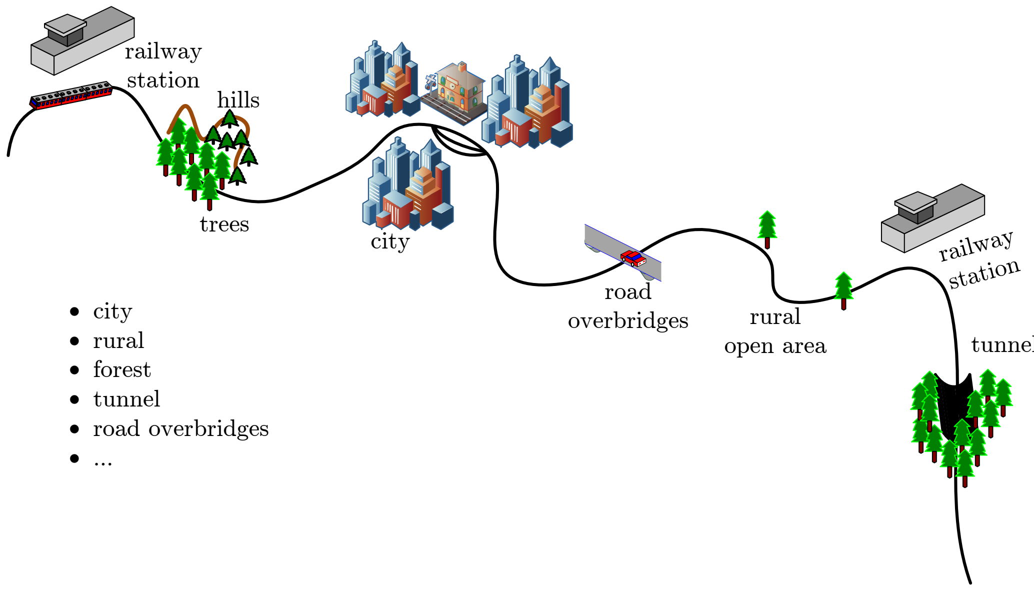


FIGURE 4.10: Environmental Scenarios Along the Track

TABLE 4.4: Railway Track Environmental Scenarios

No.	Scenario	Scenario Description
1	open area	track laying outside town or city, very good view of tracks
2	forest	track immersed in the trees
3	urban	track very close to the buildings
4	tunnel	track totally covered by a dome
5	t-cross	track laying under a railway or road bridge
6	mountainous	track with mountains on one side or close to one steep mountain or canyons causing bad satellite geometry
7	stations	many tracks, track close to the buildings

city area thus having multipath effect and bad DOP values due to canyon effects. The accuracy of GNSS receiver locations are highly related to where the train is.

The environmental scenarios can be categorised and defined as in Table 4.4. The GNSS receiver location performance varies a lot in these environments. To apply GNSS for train localisation, the safety aspects of these environments need to be analysed individually.

The GNSS receivers in these environmental scenarios will bring different GNSS receiver location measurement accuracy levels thus affecting the qualitative and quantitative quantities for the performance of the receiver. They are analysed individually in Chapter 6.

One merit for railway using GNSS is that the trains are running on the tracks. With the sufficient information stored in the digital track map, the specific environmental scenario can be recognised and the corresponding safety functions can be performed.

4.4 GNSS Performance Requirements from Service Provider Side

The GNSS performance requirements proposed by plans or standards are highly related to the organisation who formulate them. The GNSS control segment is required to control the space segment to provide signals. The GNSS performance issued from the service provider side is with the assumption that the signal reception environment is good to receive the signals, so they are considering the **S**ignal **i**n **S**pace (SIS) more than on the earth surface. This section introduces the performance requirements from the service provider side, as GPS, Galileo, and EGNOS.

4.4.1 GPS SPS SIS Performance Standard

The GPS **S**tandard **P**ositioning **S**ervice (SPS) is a localisation and timing service provided by a way of ranging signals broadcast at the GPS L1 frequency. The L1 frequency, transmitted by all satellites, contains a coarse/acquisition (C/A) code ranging signal, with a navigation data message, that is available for peaceful civil, commercial, and scientific use [22].

The GPS SPS performance is specified in terms of minimum performance standards for each performance property (accuracy, continuity, availability, and integrity). The standard provides a definition of the properties of GPS performance that, when combined with a signal reception environment and assumptions concerning the GPS receiver, allows users to define for themselves the end performance values and units they can expect for their particular applications [22].

Definition 4.3 GPS SPS SIS Accuracy (from [22])
The SPS SIS accuracy standard of GPS applies to the SIS portion of GPS error budgets for the UERE. There are four main characteristics of SPS SIS accuracy. The standards for each of these characteristic are given in this section. The four main characteristics are:

- the pseudorange data set accuracy (i.e., **U**ser **R**ange **E**rror (URE))

- the time derivative of the URE (i.e., **U**ser **R**ange **R**ate **E**rror (URRE))
- the second time derivative of URE (i.e., **U**ser **R**ange **A**cceleration **E**rror (URAE))
- the **UTC O**ffset **E**rror (UTCOE)

Each of the four main characteristic of SPS SIS accuracy is addressed in terms of "global average" performance standard. All of the SPS SIS performance standards in this section are expressed at 95% probability level.

With the URE, the accuracy of user range is also defined as **U**ser **R**ange **A**ccuracy (URA). The URA is a conservative representation of each satellite's expected **R**oot **M**ean **S**quare (RMS) URE performance based on historical data over the curve fit interval.

Definition 4.4 GPS SPS SIS Continuity (from [22])
The SPS SIS continuity for a healthy SPS SIS is the probability that the SPS SIS will continue to be healthy without unscheduled interruption over a specific time interval.

So the characteristic of continuity is defined as a kind of probability. The characteristic of continuity according to Definition 4.4 is shown in Equation 4.9.

$$Continuity = P(healthy\ SPS\ SIS)|_{specific\ time\ interval} \tag{4.9}$$

Definition 4.5 GPS SPS SIS Availability (from [22])
The SPS SIS availability is the probability that the slots in the GPS constellation will be occupied by satellites transmitting a traceable and healthy SPS SIS. So there are two characteristics for SPS SIS availability:

- Per Slot Availability: The fraction of time that a slot in the GPS constellation will be occupied by a satellite that is transmitting a traceable and healthy SPS SIS.
- Constellation Availability: The fraction of time that a specified number of slots in the GPS constellation are occupied by satellites that are transmitting a traceable and healthy SPS SIS.

The two characteristics are related. The per-slot availability depends primarily on the satellite design and the control segment procedures for on-orbit maintenance and failure response. The constellation availability depends primarily on the per-slot availability coupled with the satellite launch policies and satellite disposal criteria. From the service provider side, the formalised characteristic of constellation availability can be interpreted as:

$$Constellation\ Availability = \frac{time\ > 21\ slots\ transmitting\ traceable\ healthy\ SIS}{total\ time} \tag{4.10}$$

Definition 4.6 GPS SPS SIS Integrity (from [22])
For a PNT system, integrity is defined as the trust which can be placed in the correctness of the PNT information provided by the system. Integrity includes the ability of that system to provide timely alerts when it should not be used for PNT. The SPS SIS should not be used when it is providing **M**isleading **S**IS **I**nformation (MSI), where the threshold for misleading is a not-to-exceed tolerance on the SIS URE. The three characteristics for integrity are:

- Probability of A Major Service Failure: The probability that the SPS SIS's instantaneous URE exceeds the not-to-exceed tolerance.
- Time to Alarm: Time from the onset of MSI until an alarm indication arrives at the receiver's antenna.
- SPS URE Not-to-exceed Tolerance: The tolerance is ±4.42 times the upper bound on the URA value.

The probability of a major service failure is most of the times called "**integrity risk**" as the characteristic for integrity. And the formalised characteristic of integrity risk is defined as:

$$Integrity\ Risk = P(URE > not\text{-}to\text{-}exceed\ tolerance) \tag{4.11}$$

Based on the definition of the four properties and the related characteristics, the quantitative requirements for GPS SPS SIS performance is shown in Table 4.5. Summarise Table 4.5, the attribute hierarchy interpretation of the requirements is shown in Figure 4.11.

4.4.2 Galileo High Level Definition SoL Service Performance

In Galileo high level definition document, the performance and features for SoL service are defined in the latest version of the document published in 2002 [4]. But later Galileo SoL service is cancelled. For the Galileo satellite-only services, with different operational requirements that have been grouped around the following five reference services:

Table 4.5: GPS SPS SIS Performance Standard for Single Frequency C/A Code

Property	Characteristic	Quantity Definition (Value & Unit) in the Standard
Accuracy	URE	$\leqslant$ 7.8 m, 95% global average URE over any 3-second interval during normal operation over all AODs* and others
	URRE	$\leqslant$ 0.006m/sec, 95% global average URRE over any 3-second interval during normal operation at any AOD
	UARE	$\leqslant$ 0.002 m/sec/sec, 95% global average URAE over any 3-second interval during normal operation at any AOD
	UTCOE	$\leqslant$ 40 nsec, 95% global average UTCOE during normal operation at any AOD
Continuity		$\geqslant$ 0.9998 probability over any hour of not losing the SPS SIS availability from a slot due to unscheduled interruption.
Availability	Per-Slot	$>$ 0.957 probability that a slot in the baseline 24-slot configuration will be occupied by a satellite broadcasting a healthy SPS SIS
	Constellation	$\geqslant$ 0.98 probability that at least 21 slots out of the 24 slots will be occupied either by a satellite broadcasting a healthy SPS SIS in the baseline 24-slot configuration or by a pair of satellites each broadcasting a healthy SPS SIS in the expanded slot configuration
Integrity		$\leqslant 1 \times 10^{-5}$ probability over any hour of the SPS SIS instantaneous URE exceeding the NTE** tolerance without a timely alert during normal operations

** AOD: Age of Data, ** NTE: not-to-exceed*
URE NTE tolerance defined to be ±4.42 times the upper bound on the URA value.
This table is excerpted from the GPS SPS SIS standard [22].

- Galileo Open Service (OS)
- Safety of Life (SoL)
- Commercial Service (CS)
- Public Regulated Service (PRS)
- Support to Search and Rescue service (SAR)

Among the five reference services, the target market for the SoL service are safety critical users, whose applications or operations require stringent performance levels [4]. Like the GPS SPS SIS standard, the Galileo service will commit to provide the quality of the SIS to achieve the specified service at end-user level. The provision

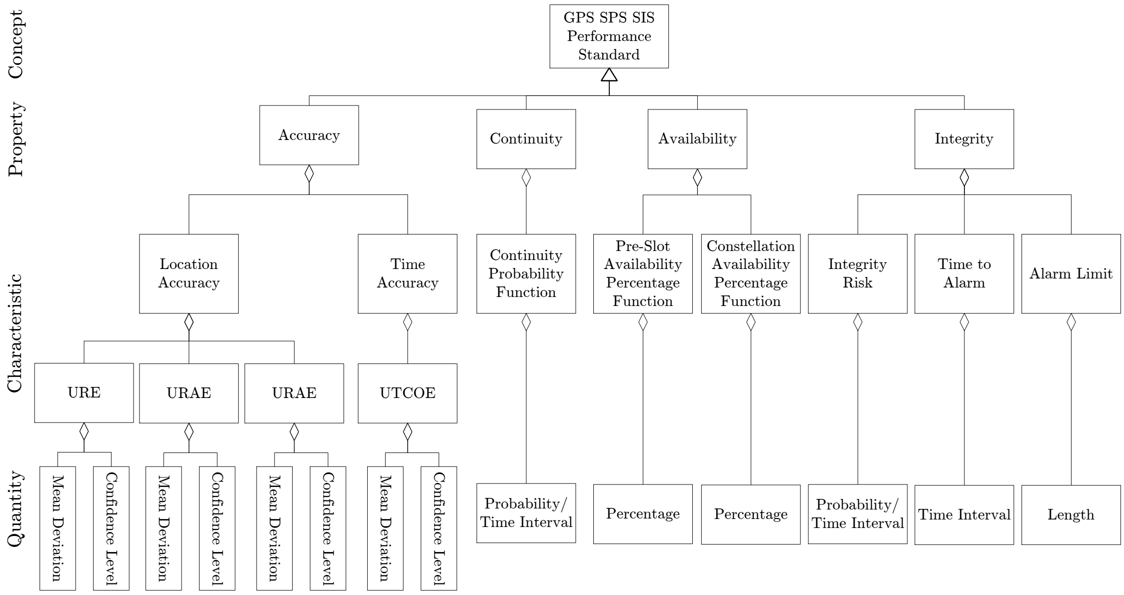


FIGURE 4.11: GPS SPS SIS Performance in Attribute Hierarchy

TABLE 4.6: Service Performance for Galileo Safety of Life Service

Property	Characteristic	Value and Unit	
		Critical Level	Non-critical Level
Accuracy	Horizontal (95%)	4 m	220 m
	Vertical (95%)	8 m	
Continuity	Continuity Risk	10^{-5}/ 15 s	10^{-4}/ h to 10^{-8}/ h
Availability		99.8%	99.8%
Integrity	Alarm Limit Horizontal	12 m	556 m
	Alarm Limit Vertical	20 m	
	Time to Alarm	6 sec	10 sec
	Integrity Risk	3.5×10^{-7}/ 150 sec	10^{-7}/ h

The Galileo SoL service is on three frequencies L1, E5a, and E5b.
This table is remade from the Galileo definition document page 16 [4].

of integrity information at global level is the main characteristic of this service. The intention of the Galileo SoL service is to provide globally according to the performances indicated in Table 4.6.

Comparing the performances of Galileo SoL in Table 4.6 and GPS SPS SIS standard in Table 4.5, the accuracy of GPS SPS SIS has been defined from both time and location sides, the accuracy of Galileo SoL service has been defined only from location side. The Galileo SoL performance is defined under two levels: critical level and non-critical level. The two levels cover two conditions of risk exposure and are applicable to many applications in different transportation domains. The critical level covers time critical operations for example, in the aviation domain approach operations with vertical guidance. The non-critical level covers extended operations that are less time critical, such as open sea navigation in the maritime domain [4].

4.4.3 EGNOS SoL Service Performance Characteristics

EGNOS has been designed to support different types of civil aviation operations. EGNOS has a very detailed definition of SoL service and as one of its key features for Europe. The EGNOS service definition document - open service defines the performance only in accuracy. This document was published in 2009 [129]. But this document is not addressing EGNOS SoL service performance. So EGNOS open service is only intended for non safety-related purposes, i.e. purposes that have no impact on the safety of human life and where a failure in accuracy, continuity, availability, or integrity of the EGNOS SIS could not cause any kind of direct or indirect personal damage, including bodily injuries or death.

In March 2011, the European Commission launched the EGNOS SoL service for aviation [130]. Then in the same time the SoL service definition document was also published [5]. Till the time of writing this dissertation, a second version was published in June 2013 [131]. One thing needs to mention, the Galileo SoL service is intended for all means of transportation. But the main objective of the EGNOS SoL service is to support civil aviation operations from en-route to **L**ocaliser **P**erformance with **V**ertical guidance (LPV) (LPV is part of the APV [132]). However, the SoL service is also intended to support applications in a wide range of other domains such as maritime, railways and road. So the characteristics of EGNOS SoL services are related to aviation terms. So the performance of EGNOS is a service provider side performance characteristic, but highly orientated for specific user applications.

EGNOS SoL adopted some guidelines from the aviation user requirements (will be stated in the next section), and the derived quantities are shown in Table 4.7. The minimum performance in the table is conservatively made since it has been taking account of a number of degraded conditions or abnormal environmental conditions, that could be experienced throughout the lifetime of the system [131].

The Galileo performance and the EGNOS performance are sharing the same structure of the properties. But the Galileo performance contains alarm limit. Since the EGNOS performance characteristic is estimated as the performance itself, the alarm limit is related to the application itself. Based on this understanding, the

TABLE 4.7: EGNOS SoL Minimum Service Performance Characteristics

Property	Characteristic	Value and Unit	Comments
Accuracy	Horizontal (95%)	3 m	Accuracy varies at
	Vertical (95%)	4 m	different locations
Continuity	Continuity Risk	$1 \times 10^{-4}/h$	NPA: 1 - $5 \times 10^{-4}/h$
		to $1 \times 10^{-8}/h$	APV-I: 1 - 5×10^{-4}/15 sec
Availability		0.99 to 0.99999	99.9% for NPA, 99% for APV-I
Integrity	Time to Alarm	less than 6 sec	
	Integrity Risk	2×10^{-7}/ 150 sec	

NPA: non precise approach, APV-I: approach procedure with vertical guidance
This table is excerpted from EGNOS SoL document [131].

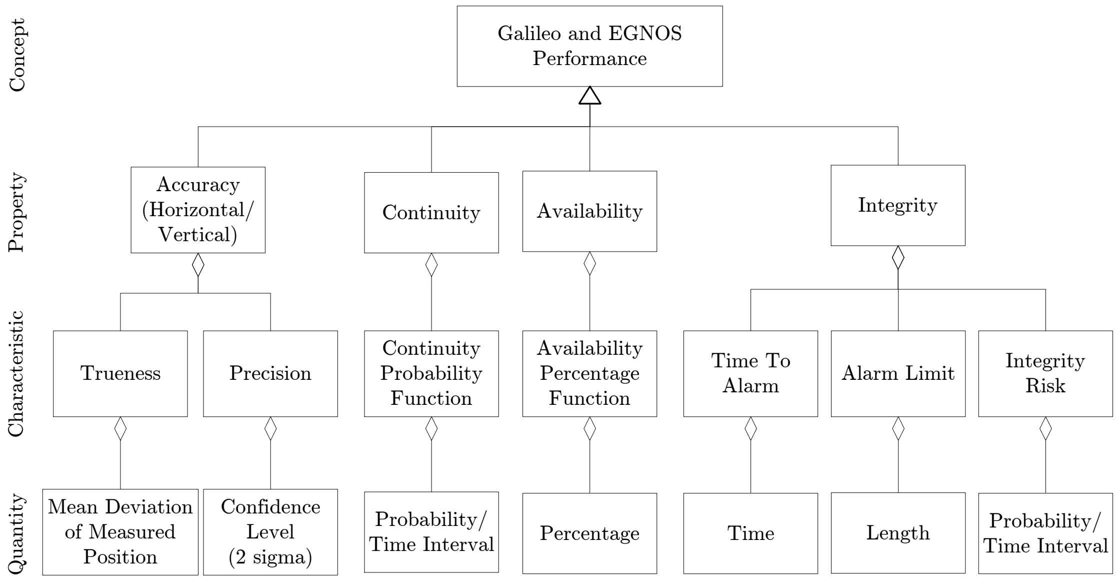


FIGURE 4.12: Galileo and EGNOS Performance in Attribute Hierarchy

Galileo and EGNOS performance can use the same attribute hierarchy structure, the performance is illustrated in Figure 4.12.

4.5 GNSS Performance Requirements from User Side

The GNSS performance requirements from the user side are more concerning about the application scenarios and the corresponding functions of the GNSS-based system, thus provide more specific values for different application scenarios.

4.5.1 PNT Performance Requirements in General

The **F**ederal **R**adionavigation **P**lan (FRP) reflects the official PNT policy and planning for the federal government of USA. The FRP covers both terrestrial and space-based, common use, federally operated PNT systems. The systems and services addressed by FRP include: GPS, augmentation to GPS, etc. [133]. So the requirements proposed by FRP are representing the requirements of the user segment in different domains for various applications. The definition of the properties in FRP PNT requirements are the basis to understand the requirements proposed in other standards and specifications.

Definition 4.7 Accuracy (from [133])
The degree of conformance of the measured location with conventional true position of the craft (vehicle, aircraft, vessel) at the given time. In general, PNT accuracy performance depends on the quality of the pseudorange and carrier phase measurements as well as the broadcast navigation data.

When specifying linear accuracy, or when it is necessary to specify requirements in terms of orthogonal axes (e.g., along-track or cross-track), the 95% confidence level (2σ) will be used. When two-dimensional accuracies are used, the 2 drms uncertainty estimate will be used. The 2 drms is twice the radial error drms. The radial error is defined as the root-mean-square value of the distances from the point of the location fixes to a collection of location measurements. The distribution of the error is normally elliptical. As the error ellipse collapses to a line the confidence level of the 2 drms measurement approaches 95%; as the error ellipse becomes circular, the confidence level approaches 98%.

Specifications of PNT system accuracy generally refers to one or more of the following types of the characteristics:

- Predictable Accuracy: The accuracy of a PNT system's location solution with respect to the charted solution. Both the location solution and the chart must be based upon the same geodetic datum.
- Repeatable Accuracy: The accuracy which a user can return to a location whose coordinates has been measured at a previous time with the same PNT system.
- Relative Accuracy: The accuracy with which a user can measure location relative to that of another user of the same PNT system at the same time.

Definition 4.8 Continuity (from [133])
The continuity of a system is the ability of the total system (comprising all elements necessary to maintain an aircraft position within the defined airspace) to perform its function without interruption during the intended operation. More specifically, continuity is the probability that the specified system performance will be maintained for the duration of a phase of operation, presuming that the system was available at the beginning of that phase of operation. The level of the continuity provided by PNT thus varies with the specific performance requirements for any given application.

So the characteristic of continuity is defined as the ability of the total system, which is represented by the probability of a function. Mathematically the characteristic of continuity is defined as:

$$Continuity = P(maintained\ system\ performance)|_{phase\ of\ operation\ \&\ duration} \tag{4.12}$$

Definition 4.9 Reliability (from [133])
The reliability of a PNT system is a function of the frequency with which failures occur within the system. It is the probability that a system will perform its function within defined performance limits for a specified period of time under given operating conditions. Formally, reliability is one minus the probability of system failure.

The characteristic of reliability is also defined as a probability function. The mathematical interpretation for reliability characteristic is:

$$Reliability = 1 - P(system\ failure)|_{specified\ function\ \&\ time} \tag{4.13}$$

Definition 4.10 Availability (from [133])
The availability of a PNT system is the percentage of time that the services of the system are usable. Availability is an indication of the ability of the system to provide a usable navigation service within a specified coverage area. Availability is a function of both the physical characteristics of the environment and the technical capabilities of the transmitter facilities.

So the characteristic of availability is defined as a percentage function. The characteristic of availability can be interpreted as:

$$Availability = \frac{time\ PNT\ service\ usable}{total\ time}|_{specified\ coverage\ area} \tag{4.14}$$

TABLE 4.8: FRP Surface Transportation PNT User Requirements

Property Characteristic	Accuracy * (m) 95%	Continuity	Availability	Integrity AL** (m)	Integrity TTA*** (sec)
navigation and route guidance	1 - 20	****	> 95%	2 - 20	5
automated vehicle monitoring	0.1 - 30	****	> 95%	0.2 - 30	5 - 300
automated vehicle identification	1	****	99.7%	3	5
public safety	0.1 - 30	****	95 - 99.7%	0.2 - 30	2 - 15

** Trueness as Accuracy Characteristic, ** AL: Alarm Limit, *** TTA: Time to Alarm*
***** Continuity applies to operations phases, not defined for surface transportation.*
The requirements are excerpted from the table on FRP page 4-28 [133].

Definition 4.11 Integrity (from [133])
Integrity is the measure of the trust that can be placed in the trueness of the information supplied by a PNT system. The characteristic of integrity includes the ability of the system to provide timely warnings to users when the system should not be used for navigation.

Remark 4.1 Ambiguity of Reliability and Continuity
From the definitions of reliability and continuity, the Equation 4.13 and Equation 4.12 shows the $P(system\ failure)$ and $P(maintained\ system\ performance)$ for "its function for a specific period of time" or "the duration of a phase of operation" with the accordance of "defined performance limits" or "specified system performance". Currently in both GNSS and airborne requirements or standards, the continuity is always used instead of reliability. But railway standards issues reliability. The relation and difference between reliability and continuity are discussed and formally represented in Chapter 6 Section 5.3 later.

In FRP, there are different user requirements for different applications. For surface transportation, the requirements of highway and railway are defined together [133]. As seen from the requirements listed in Table 4.8, the reliability is not required at all; and the continuity are just mentioned, the values are still not defined.

Comparing the four categories of the applications, the accuracy requirement and the integrity requirement are sort of related. Basically, the alarm limit is always greater than the accuracy requirement. The accuracy level is highly related to the purpose of the application.

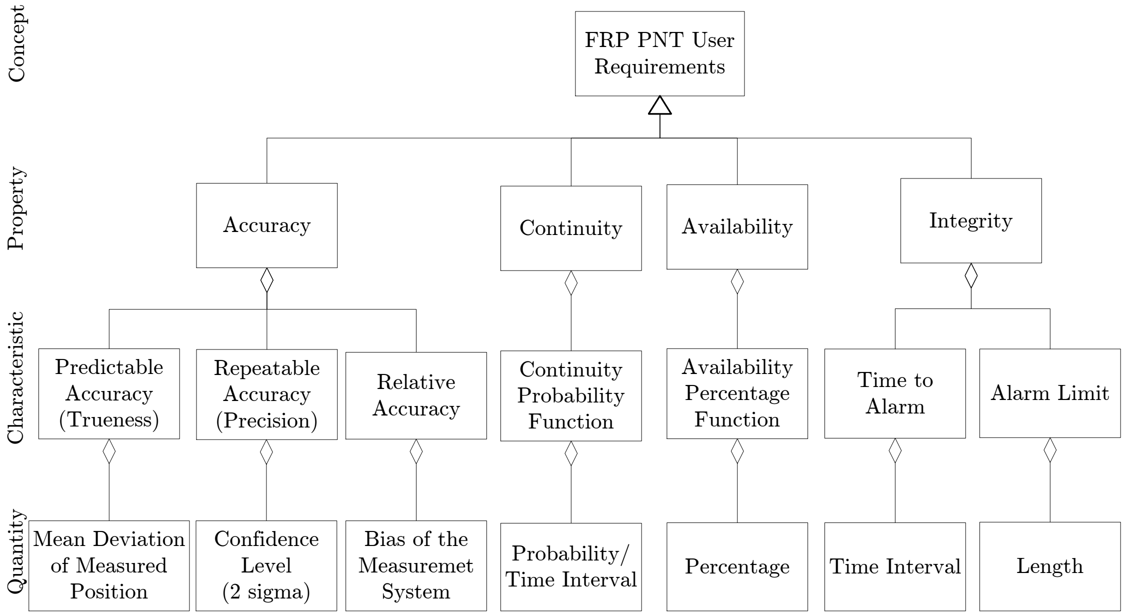


FIGURE 4.13: FRP User Requirements in Attribute Hierarchy

Based on the four properties of PNT performance requirements from FRP and the attribute hierarchy for the properties, the surface user requirements according to the properties and characteristics defined above are shown in Figure 4.13 as stated in FRP.

4.5.2 RTCA GNSS Performance for Airborne Equipments

The DO-229D issued by RTCA provides standards for single frequency airborne navigation equipment. The standards are intended to be applicable for GPS and also other SBAS such as WAAS and EGNOS [64]. The RTCA GNSS performance for airborne equipment properties also includes accuracy, continuity, availability, and integrity. The definition of these properties are inherited from FRP ones. But the characteristics for these four properties are defined in a more extended way. Besides the FRP characteristics, the integrity property for RTCA GNSS performance also includes continuity risk and protection limit.

Definition 4.12 Continuity Risk (from [134])
Continuity risk is the probability that the system will not provide guidance information with the accuracy and the integrity required for the intended operation.

The symbol for continuity risk is represented by $CR(t)$. Meanwhile, the symbol of continuity is represented by $C(t)$. The characteristic of both are denoted by

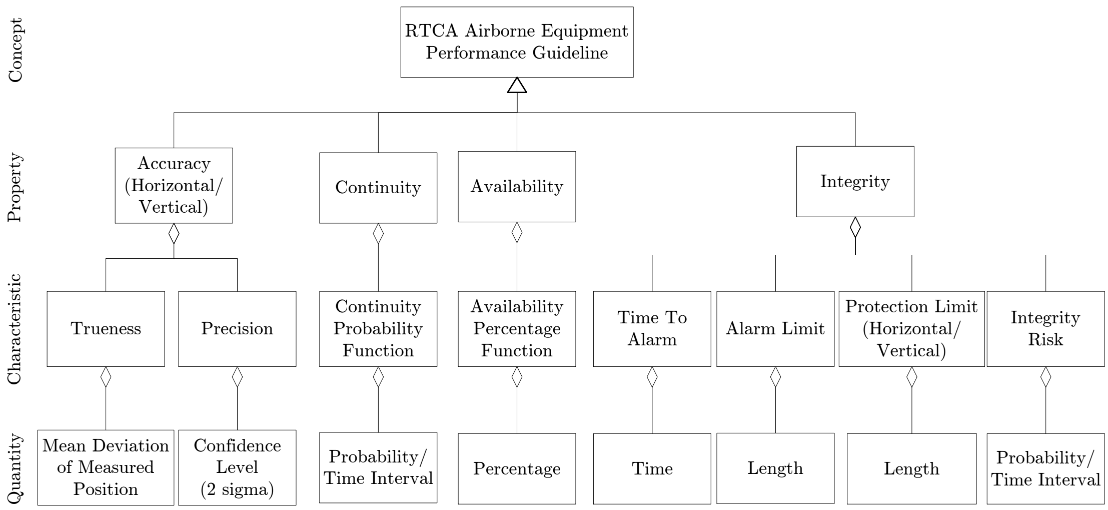


FIGURE 4.14: RTCA Airborne Equipment Performance in Attribute Hierarchy

probability of functions, the sum of both is 1.

$$CR(t) + C(t) = 1$$

The characteristics for integrity property also have more meanings than both FRP requirements and GPS SPS SIS performance standard. The integrity property contains another characteristic called protection limit along with the defined alarm limit in last section. The protection limit contains both **H**orizontal **P**rotection **L**imit (HPL) and **V**ertical **P**rotection **L**imit (VPL). The most related protection limit for this dissertation is HPL, since the GNSS for train localisation is applied on the earth surface.

Definition 4.13 Horizontal Protection Limit$_{Fault\ Detection}$ (from [64])
The Horizontal $Protection\ Limit_{Fault\ Detection}$ (HPL_{FD}) is the radius of a circle in the horizontal plane (the local plane tangent to the WGS-84 ellipsoid), with its centre being at the true position, that describes the region assured to contain the indication horizontal position. It is a horizontal region where the missed alarm and false alarm requirements are met for the chosen set of satellites when autonomous fault detection is used. It is a function of the satellite, user geometry and the expected error characteristics: it is not affected by actual measurements. Its value is predictable given reasonable assumptions regarding the expected error characteristics.

So the definitions above together with other properties in FRP can be now expressed as a new attribute hierarchy structure in Figure 4.14.

Table 4.9: ICAO GNSS Performance Requirements (Excerpted)

Property	Characteristic	en-route	APV-I
Accuracy	Horizontal Accuracy (95%)	3.7 km	16 m
	Vertical Accuracy (95%)	N/A	6 - 4 m
Continuity	Continuity Risk	1×10^{-4}/ h to 1×10^{-8}/ h	8×10^{-6} per 15 sec
Availability		0.99 to 0.99999	0.99 to 0.99999
Integrity	Integrity Risk	1×10^{-7}/ h	2×10^{-7}/ 150 sec
	Horizontal Alarm Limit	1.85 - 7.4 km	40 m
	Vertical Alarm Limit	N/A	20 m
	Time to Alarm	10 sec - 5 min	6 sec

N/A: not available
The requirement is excerpted from the ICAO recommendations [134].

Since RTCA itself is not an agency of any country, its documents are treated as guidelines not as quantitative requirements. Under the administration of RTCA, the ICAO published the requirement for GNSS, SBAS, and GBAS for en-route through category I precision approach. Six categories for SIS performance requirements are provided. The combination of GNSS elements and a fault-free GNSS user receiver shall meet the signal-in-space requirements defined in Table 4.9 [134].

Notice that, the requirements call for horizontal accuracy and horizontal alarm limit for en-route, but conversely calls for vertical accuracy and vertical alarm limit for APV-I approaching and other APV modes. So vertical accuracy is requested in near terminal operations.

4.5.3 GNSS for Railway Application Performance Advisory

Considering the performance requirements by FRP for surface transportation in Table 4.8 and the performance guideline by RTCA for airborne equipments in Table 4.9, there are also some advisories for the applications in railway safety-related applications in different kind of railway lines [135]. The advisory for the railway safety-related applications is shown in Table 4.10. Basically this advisory follows the structure for the airborne equipments proposed by RTCA. As also mentioned in the notes of Table 4.10, the integrity risk is also required for accomplishing the safety-related functions in railway domain.

Table 4.10: GNSS Requirements Advisory for Railway Applications

Applications	I ATC on high density line	II train control on medium density line	III train control on low density line
Horizontal Accuracy (m, 95%)	1	10	25
Continuity	>99.98%	>99.98%	>99.98%
Availability	>99.98%	>99.98%	>99.98%
Fix Rate (sec)	1	1	TBD
Alarm Limit (m)	2.5	20	50
Time to Alarm (sec)	<1.0	<1.0	<1.0

For efficient use in architectures accomplishing safety-related functions integrity risk should be added.
This table is remade from the table in requirements of rail applications Page 13 [135].

Similar to the other user side requirements and guidelines, the railway application performance advisory also starts from the accuracy requirement. Then the continuity, availability, and also integrity requirements are proposed based on it. But the GNSS for railway performance advisory only calls for horizontal accuracy and integrity requirements. Instead of continuity risk requested the RTCA airborne equipment performance guidelines, the opposite side characteristic continuity is stated by the GNSS railway application performance advisory. Besides, the integrity risk is not mentioned in the advisory. The attribute hierarchy structure for the advisory properties and related characteristics is shown in Figure 4.15.

4.6 Chapter Summary

This chapter defines the important terms used in this dissertation (position, positioning, location, localisation). After a clear comparison and a formal illustration of the relation between the terms, the appropriate terms applied in the following chapters are fixed.

After that, the GNSS, the GNSS-based localisation unit, and the evaluation purpose established reference measurement system are introduced accordingly. These three systems are used, applied, investigated, evaluated, and verified in the following chapters. Since the GNSS receiver is a vital component for the systems, the

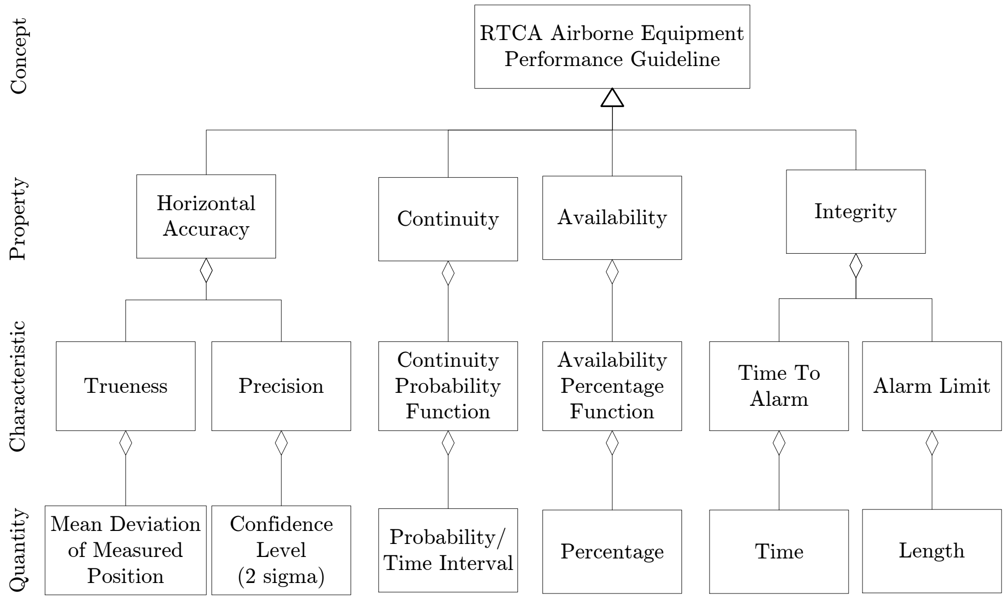


FIGURE 4.15: GNSS Performance Advisory for Railway Applications in Attribute Hierarchy

localisation principles of GNSS, the environmental affection of the accuracy are also introduced.

The evaluation and the verification of GNSS for train localisation are all based on the clear and correct understanding of the GNSS performance attributes. So the related existing GNSS requirements from both the service provider side and the user side are interpreted in the same form by the attribute hierarchy for the definition of the properties, characteristics, quantities, and corresponding values. The exact value and unit for each characteristic is also illustrated in the tables.

Chapter 5

GNSS for Train Localisation Performance Properties Migration

GNSS performance properties have been intensively illustrated in Chapter 4. Railway applications need to demonstrate RAMS as required. GNSS for train localisation converges both GNSS and RAMS performance properties. The migration of both performance properties is to propose the new performance properties fitting GNSS for train localisation.

5.1 Relation between GNSS Performance Properties

In Chapter 4, GNSS performances are stated from the service provider side (Section 4.4) and the user side (Section 4.5). Although the stated GNSS performances offer the same properties in the attribute hierarchy structure, but the characteristics and the following quantities in values and units are having many differences. This section analyses these GNSS performances, and then compares these GNSS performance requirements quantitatively, finally the relations between the properties are analysed.

5.1.1 Comparison of GNSS Performance Requirements from Both Sides

The GNSS performance requirements from the service provider side issue the performance in a more general way. The GPS SPS SIS standard issues the requirement with a signal reception environment and assumption to allow users to define themselves the end performance they can expect for their particular applications [22].

Table 5.1: Summary of GNSS Performance Categories from Service Provider Side

Service Provider Side	Categories
GPS SPS SIS [22]	no categories, applications need to define for themselves
Galileo SoL service [4]	critical and non-critical
EGNOS SoL service [131]	NPA and APV

The Galileo high level definition only considers two categories: critical and non-critical. Besides, EGNOS SoL is to support civil aviation operations in both non precision approach (NPA) and approach with vertical guidance (APV). A summary of the categories for the GNSS performance from the service provider side is listed in Table 5.1. The GNSS performances proposed from the service provider side are aiming at providing enough SIS performance not considering user application and environmental scenarios. It allows the user to define the requirement values for specific applications.

The GNSS performance requirements from the user side are raised for a lot of specific application scenarios. The GPS FRP is the general plan for aviation, maritime, road, and railway domains. Each domain has defined many application scenarios. For example, as shown in Table 4.8, 11 application scenarios have been specified for surface transportation. And also, the RTCA recommendation sets 6 application scenarios for GNSS performances as the necessary safety-related application scenarios. Even the GNSS performance advisory from the railway side, as shown in Table 4.10, the performance is roughly categorised into three application scenarios. A summary of the application scenarios in these three documents is listed in Table 5.2.

From the content of Table 5.1 and Table 5.2, the GNSS performance requirements from the user side specify the performance much more in detail for their own needs. The values of the properties in each requirement are specific for each application. So the values of the properties in GNSS for train localisation should also be clearly specified. This starts from understanding of the properties.

5.1.2 GNSS Performance Properties and Values

Even though the GNSS performance requirements values are raised differently for many applications, they still follow similar attribute hierarchy structure. With a comparison of the attribute hierarchy of the GNSS performance requirements, only

TABLE 5.2: Summary of GNSS Performance Application Scenarios from User Side

User Side	Application Scenarios
FRP [133]	1. space: on-board autonomous navigation, earth observation satellites, altimety missions, occultation measurements (4 applications)
	2. aviation: oceanic, en-route, terminal, NPA, APV-I, APV-II, CAT I (7 applications)
	3. maritime: inland waterway phase, harbour entrance and approach phase, coastal phase, ocean phase(4 phases)
	4. surface: navigation and route guidance, automated vehicle monitoring, automated vehicle identification, public safety, resource management, collision avoidance, geophysical survey, geodetic control, accident survey, emergency response, intelligent vehicle initiative (highway, 11 applications); positive train control (transit, 1 application)
	5. others: geodesy and surveying, mapping, charting, geographic information systems (GIS), agriculture and natural resources applications, geophysical applications, meteorological applications, timing and frequency (7 applications)
RTCA [64] [134]	en-route, en-route terminal, NPA, APV-I, APV-II, CAT I (6 application scenarios)
Railway Advisory [135]	ATC on high density line, train control on medium density line, train control on low density line (3 application scenarios)

four properties are stated in the requirements quantitatively. They are **accuracy**, **continuity**, **availability**, and **integrity**. So these four properties can be treated as the necessity of GNSS performance properties.

With the four properties, each GNSS performance document extends them into similar characteristics and then different values are proposed. A comparison of the values of them based on the same properties and characteristics are listed in Table 5.3. The values in the table for each document is using only one specific application as an example, the FRP part is using the navigation and route guidance as an example, GPS SPS is using the general requirement, RTCA uses the APV-I as an example, the railway application advisory is using the medium density line as an example. As seen in the table, the unit of the continuity risk and integrity risk proposed by aviation application is different from other three risk units.

The **accuracy** property consists of two characteristics: trueness and precision. In

Table 5.3: Comparison of the Values from Different Document and Application

Characteristics	FRP* [133]	GPS SPS [22]	RTCA APV-I [134]	Railway** [135]
Horizontal Accuracy (95%)	1 - 20 m	$\leqslant$ 7.8 m	16 m	10 m
Vertical Accuracy (95%)			4 - 6 m	
Continuity Risk	TBD	2×10^{-4}/ h	8×10^{-6}/15 sec	2×10^{-4}/ h
Availability	> 95%	> 98%	99% - 99.99%	> 99.98%
Integrity Risk	TBD	1×10^{-5}/ h	2×10^{-7}/ 150 sec	TBD
Alarm Limit	2 - 20 m	34.48 m	40 m	20 m
Time to Alarm	5 sec	< 6 hour	6 sec	1 sec
Protection Limit	n.a.	n.a.	40 m	n.a.

TBD: To Be Defined, n.a.:not available

* Among the FRP applications, the navigation and route guidance is used here.

** The railway advisory uses the train control on medium density line as an example.

Table 5.3 only the trueness is written, but precision is always considered. Because the values of the trueness requirement are always under the consideration of 2σ precision level. Besides, the vertical trueness is specially required by RTCA for aviation APV-I application.

The **continuity** property is stated by all requirements. The characteristic for continuity is the continuity risk. The interesting part is some documents leave the definition to the user for its own applications. And the aviation applications define the continuity risk for APV applications in 15 seconds time span, while the other documents are define the continuity risk generally in 1 hour time span.

The **availability** property is stated by each requirement as stationary availability, the difference of them can only be shown by values. The unit is also the same, stated as %.

The last property **integrity** is described by four characteristics: integrity risk, alarm limit, time to alarm, and horizontal alarm limit. The integrity risk is, like the continuity risk, issued by all four requirements. But the unit is having several differences, similar to continuity risk, the units are in 150 seconds time span or 1 hour time span. But the alarm limit and time to alarm is defined in the same way. At last, the RTCA requirement also states the horizontal protection limit, leaving all other three empty in this characteristic.

5.1.3 Relation between the Four Properties

The most direct reflection of a GNSS-based system performance is the measurement accuracy, no matter time accuracy or location accuracy. The GNSS receiver delivers location measurements, the location measurements are in the unit of length (meters). The accuracy performance is also represented by length measurement. Thus, accuracy performance can be directly derived from the location measurements, no transformation is required.

The continuity and availability both mention the “maintained performance” in both definitions. The presence of both performances require a definition of the “maintained performance”. Since the direct measurement from the GNSS receiver is the location, the “maintained performance” needs to be defined using location accuracy performance values.

Taking integrity into consideration, in Table 5.3 the alarm limit is also defined through accuracy performance. The value of the alarm limit is always greater than the accuracy value requirement.

So the continuity, availability, and integrity characteristic values are all based on the accuracy performance value. Accuracy can be regarded as the foundation of all other three GNSS performance properties. The continuity and availability are related according to the requirement of the “maintained performance”. In this dissertation, the availability characteristic is using the stationary availability, which is a long term evaluation result. So availability is showing the performance of a long time span, continuity is showing the average performance in a specific time interval. And integrity shows the performance outside the accuracy performance value. The relation between these four properties can be shown in Figure 5.1.

Till now, the four properties are raised and considered only according to GNSS performances. In order to apply GNSS for train localisation, the GNSS performance properties need to be migrated to be identical with railway performance properties. The following section introduces the railway RAMS.

5.2 RAMS Requirements for Railway Applications

The goal of a railway system is to achieve a defined level of rail traffic in a given time, safely. Railway RAMS describes the confidence with which the system can guarantee the achievement of this goal. Railway RAMS has a clear influence on the quality with which the service is delivered to the customer. Quality of Service

FIGURE 5.1: Relation between GNSS Performance Properties

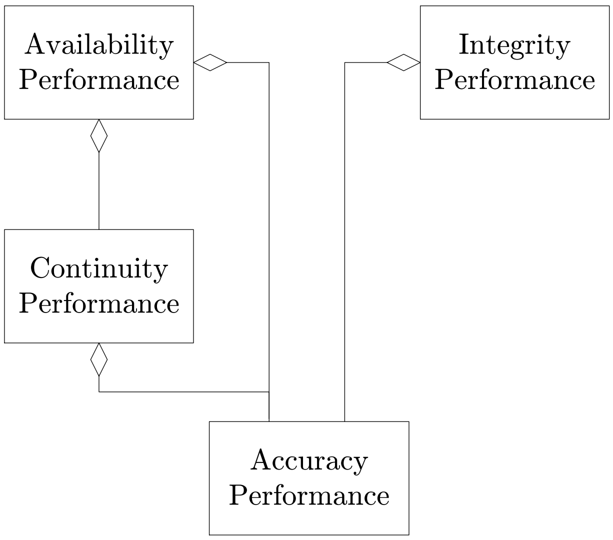
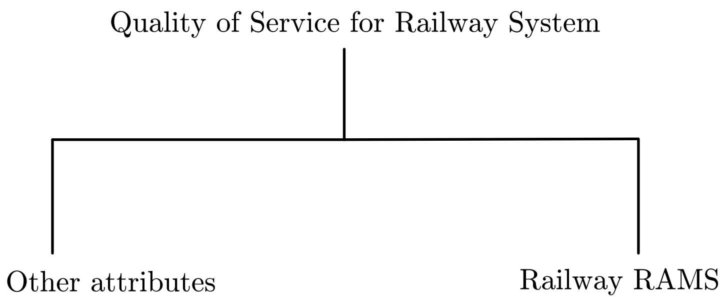


FIGURE 5.2: Relation between QoS and Railway Application RAMS [18]



is influenced by other characteristics concerning functionality and performance, for example frequency of service, regularity of service and fare structure. The relation between QoS and railway RAMS is shown in Figure 5.2. System RAMS, in the context of this European standard, is a combination of reliability, availability, maintainability, and safety [18] [86] [91]. That is in abbreviation RAMS.

RAMS is a characteristic of a system's long term operation and is achieved by the application of established engineering concepts, methods, tools and techniques throughout the lifecycle of the system. The RAMS of a system can be characterised as a qualitative and quantitative indicator of the degree that the system, or the subsystems and components comprising that system, can be relied upon to function as specified and to be both available and safe.

5.2.1 RAMS Requirements for Railway System

The definitions of the RAMS parameters are inherited from IEC 60050 standard.

Definition 5.1 Reliability (from [136])
The probability that an item can perform a required function under given conditions for a given time interval (t1, t2).

Reliability is normally represented by $R(t)$ or by the compliment of R(t). The compliment is represented by F(t), where $F(t) = 1 - R(t)$. Since $R(t)$ is a probability, normally the $R(t)$ is related to failure rate $\lambda(t)$, where $\lambda(t) = dF(t)/dt$. When the failure rate is constant, then it is represented by λ. Then the characteristic of reliability can be estimated as

$$R(t) = e^{-\lambda T}|_{T=|t_j - t_k|} \tag{5.1}$$

Besides, **M**ean **T**ime **T**o **F**ailure (MTTF) is also used to represent the reliability performance for a repairable system. And in this background MTTF is normally calculated as:

$$MTTF = E[T_i],\ T_i = |t_j - t_k| \tag{5.2}$$

In that, T_i is a time span, and t_j and t_k are timestamps, between t_j and t_k, the item is performing its required function. For a constant failure rate λ, MTTF is used to express reliability. Normally, $MTTF = 1/\lambda$.

Definition 5.2 Maintainability (from [136])
The probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources.

Maintainability is based on the idea that the system is repairable. So the **M**ean **T**ime **T**o **R**epair (MTTR) is normally used to express the performance of maintainability. Normally, $MTTR = 1/\mu$.

Definition 5.3 Availability (from [18])
The ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided.

There are three kinds of availabilities [91], among them the stationary availability is adopted for the evaluation purpose of GNSS for train localisation in Chapter 6. The stationary availability is normally represented by the abbreviation of availability as

A, the characteristic of stationary availability is estimated by:

$$\begin{aligned} A &= \frac{MTTF}{MTTF+MTTR} \\ &= \frac{\mu}{\lambda+\mu} \end{aligned} \tag{5.3}$$

Definition 5.4 Safety (from [18])
Freedom from unacceptable risk of harm.

Safety is defined in a more abstract way. The necessity to estimate safety quantitatively calls for the safety function and safety integrity level definitions in EN 50129 [20].

Definition 5.5 Safety Function (from [15])
A safety function is defined as a function to be implemented by a safety-related system, this system is an **E**lectric/**E**lectronic/**P**rogrammable **E**lectronic (E/E/PE) system. another technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the **E**quipment **U**nder **C**ontrol (EUC), in respect of a specific hazardous event. A safety function is not part of machine operation: if such a function fails, the machine can still operate normally, but the risk of injury from its operation increases.

Definition 5.6 Functional Safety (from [15])
Functional safety is part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.

To understand the functional safety more clearly, the risk and harm and the corresponding hazard also needs to be defined.

Definition 5.7 Risk (from [18])
The probable rate of occurrence of a hazard causing harm and the degree of severity of the harm.

Formally, the characteristic of risk can be estimated by [137]:

$$Risk = probability\ rate\ of\ occurrence\ of\ harm \times severity\ of\ harm$$

Definition 5.8 Harm (from [18])
Injury or damage to the health of people, or damage to property or the environment.

Definition 5.9 Hazard (from [18] and [20])
In EN 50126, hazard is defined as a physical situation with a potential for human

Table 5.4: Tolerable Hazard Rate and SIL Relation Table [20]

Tolerable Hazard Rate (THR) per hour and per function	Safety Integrity Level (SIL)
$10^{-9} \leqslant THR < 10^{-8}$	4
$10^{-8} \leqslant THR < 10^{-7}$	3
$10^{-7} \leqslant THR < 10^{-6}$	2
$10^{-6} \leqslant THR < 10^{-5}$	1
$THR \geqslant 10^{-5}$	0

injury.

In EN 50129, hazard is defined as a condition that could lead to an accident.

Definition 5.10 Safety Integrity (from [15])
The safety integrity is defined as the likelihood of a system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

Remark 5.1 Safety Requirements Allocation and Safety Integrity Level (SIL)
Safety requirements consists of both safety function requirements and safety integrity requirements. So it is required to allocate a safety integrity level to each safety function. Safety integrity level is a discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.

In railway safety application standard EN 50129, SIL is expressed through tolerable hazard rate (THR). Having followed the measures and methods required for SIL x (x = 0, 1, 2, 3, 4) there is no requirement to consider the systematic failures when demonstrating the THR is achieved. A SIL table is shown in Table 5.4 [20]. SIL 0 means there are no safety requirement for this function.

A description of railway RAMS according to EN 50126 [18] is also made using attribute hierarchy in Figure 5.3. This structure shows the basic and necessary characteristics to be evaluated according to RAMS.

Availability distinguishes from reliability for the possibility of withstanding more service outages during the system lifetime, just one outage being unacceptable for a reliable system. Safety distinguishes from availability and reliability for the consequence of the service outage, which is ranked according to a severity level. Maintainability is the measure of the repair process including fault diagnosis, localisation

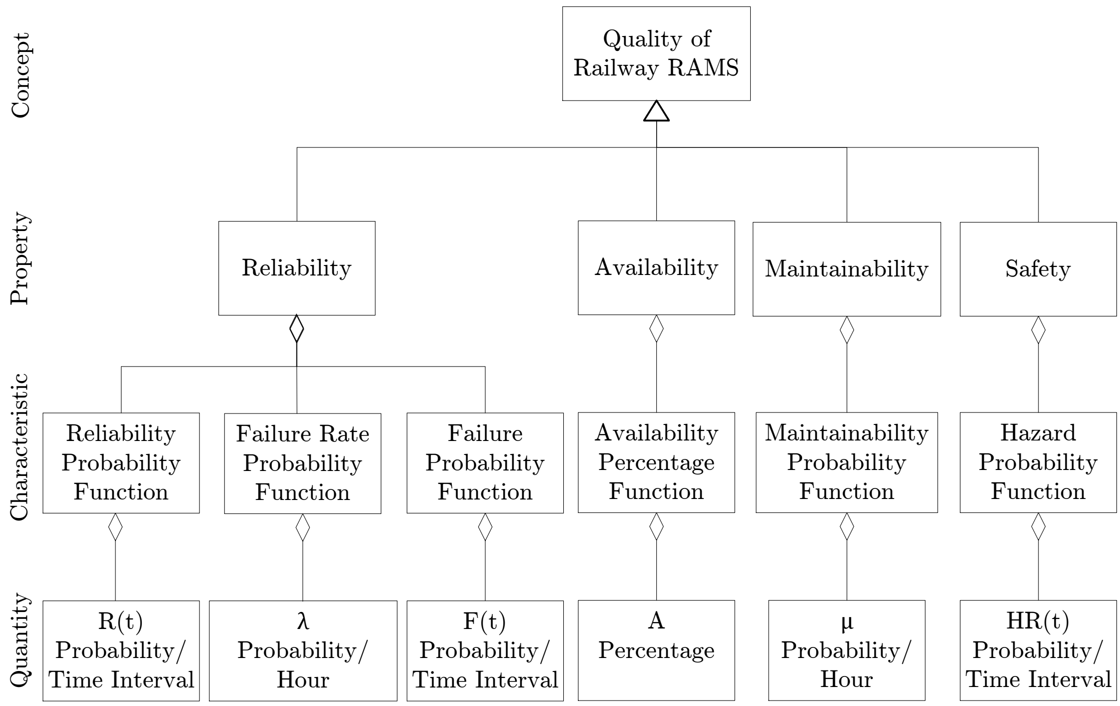


FIGURE 5.3: Railway RAMS in Attribute Hierarchy

and isolation plus repair or replacement.

5.2.2 Relation between RAMS Properties and Dependability

Definition 5.11 Dependability (from [136])
The collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance, and maintenance support performance.

Dependability is the part of the measurement for the quality of service in time given by the system. Reliability, availability and maintainability compose the dependability [138]. The relation between RAM and dependability can be shown more clearly in the attribute hierarchy in Figure 5.4.

In this dissertation, maintainability is not the concern, because GNSS maintainability is operated by the master control station belonging to the control segment. From user segment, we cannot maintain GNSS. So the dependability performance in this dissertation means reliability and availability. When no safety aspects are considered, only dependability, we need to distinguish and make clear between error, fault and failure. These are important terms for a pre-safety analysis.

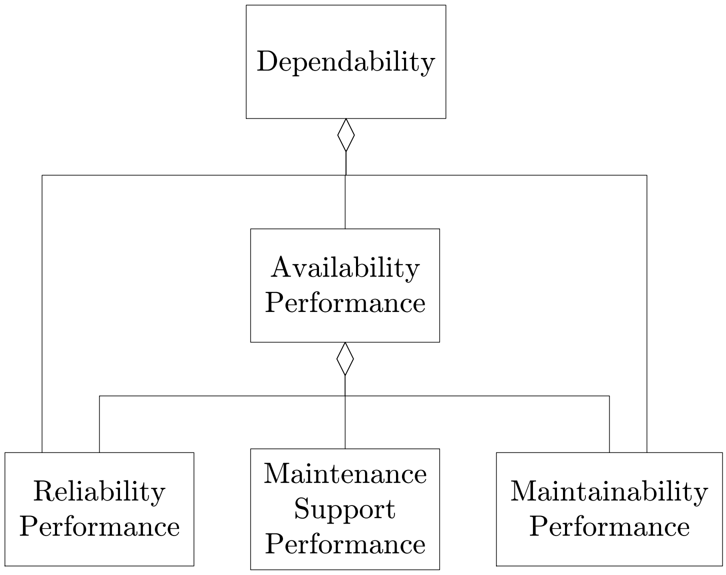


FIGURE 5.4: Dependability with RAM

Definition 5.12 Error (from [136])
A discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition.

Definition 5.13 Fault (from [136])
The state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

Remark 5.2 Fault and Faulty
In this dissertation, fault and faulty both means states. Actually faulty state is more used in this dissertation.

Definition 5.14 Failure (from [136])
The event when a required function is terminated (exceeding the acceptable limits).

So error, fault are also related to the performance, they are the results of meeting or not meeting the performance target value (requirements). The relation between them are shown in Figure 5.5 [139].

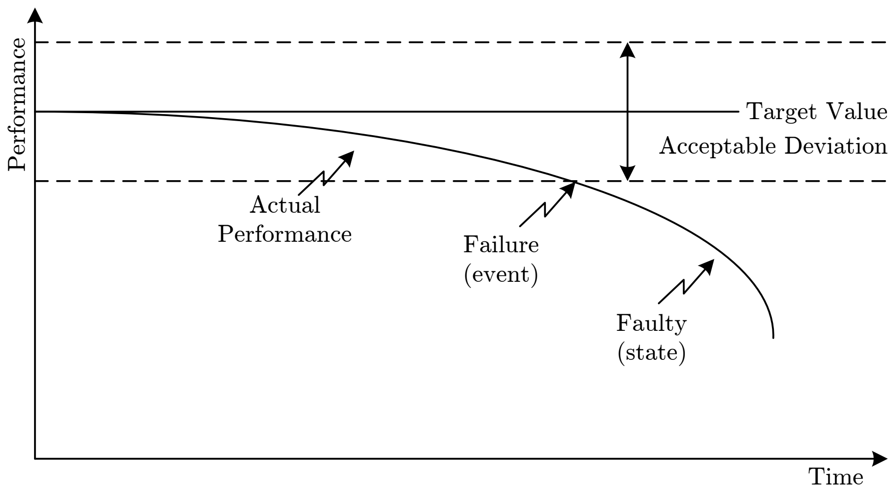


FIGURE 5.5: Illustration of the Difference between Failure and Fault [139]

5.2.3 Hazard and Risk Analysis As Part of Safety Evaluation

For hazard and risk analysis according to EN 50126 (in standard Section 4.6.2 [18]) it is the normative requirement. Hazard and risk analysis should be performed at various phases of the system lifecycle by the authority responsible for that phase and shall be documented [18].

For the whole system lifecycle, IEC 61508 sets out a generic approach for all safety lifecycle activities for systems comprised of E/E/PE components that are used to perform safety functions. A product from the beginning to the end of the lifecycle, the hazard and risk analysis is in them all. Among the lifecycle of the localisation unit, it should follow the safety lifecycle as defined in IEC 61508 [12]. The hazard and risk analysis in the lifecycle can be divided into two sub processes. They are hazard identification and risk assessment. To make the third process in the lifecycle more understandable, a extended figure is shown in Figure 5.6 [140]. Based on the definitions of risk, harm and hazard the relation between them can be shown in Figure 5.7 [87] [94].

Remark 5.3 Relation between Error, Failure, Faulty State, Hazard, and Accident
As shown in Figure 5.5, the system has an error that is the original deviation. If the deviation is bigger than acceptable deviation, a failure can occur. If the system is safety-related, the hazard identification and risk assessment process is required. Then if the hazard is not removed, then it will cause an accident, if there is an exposed body protected by law. The whole process can be shown in a Petri net as in Figure 5.8.

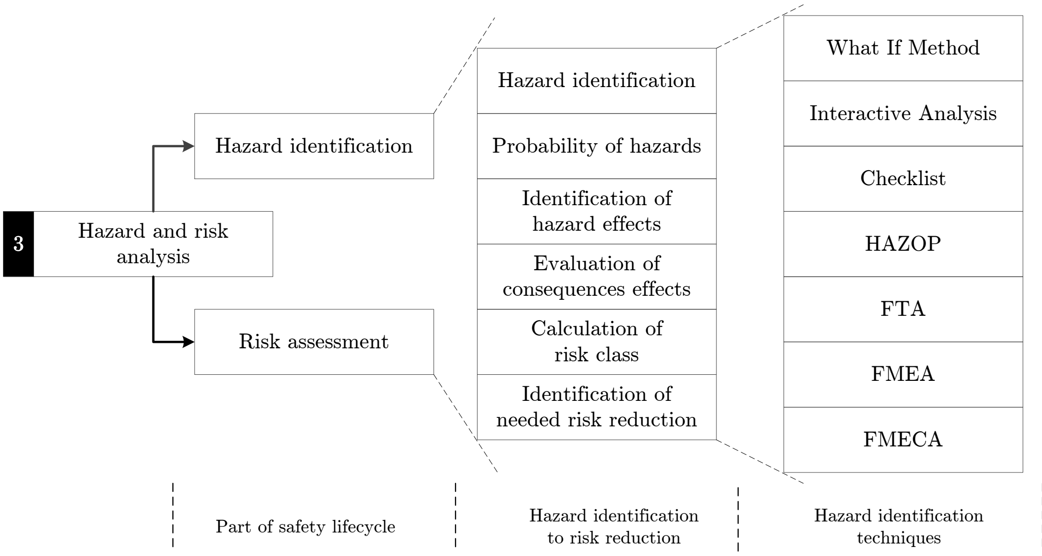


FIGURE 5.6: Detailed Hazard and Risk Analysis [140]

Safety assessment needs to identify the hazard and also the risk of the localisation unit, particularly the safety integrity level needs to be allocated. For safety evaluation, actually the risk assessment is needed. The risk assessment includes the following steps:

1. identify the hazards;
2. analyse and evaluate the risks associated with the hazards;
3. determine appropriate ways to eliminate or control of hazards.

So the risk assessment should be done according to each function of the safety-related application. Risk is always connected to safety thus safety integrity. When the level of safety for the application has been set and the necessary risk reduction estimated, the safety integrity requirements can be derived for systems and components of the application based on the risk assessment process. Safety integrity can be viewed as a combination of quantifiable elements (generally associated with hardware, i.e. random failures) and non-quantifiable elements (generally associated with systematic failures in software, specification, documents, processes, etc.). External risk reduction facilities and the system risk reduction facilities should match the necessary risk reduction required for the system to meet its target level of safety.

EN 50126 does not define the correlation between safety integrity and failure probabilities for railway systems, although it should be noted that a generic correlation is defined within draft standard IEC 61508 and also EN 50129.

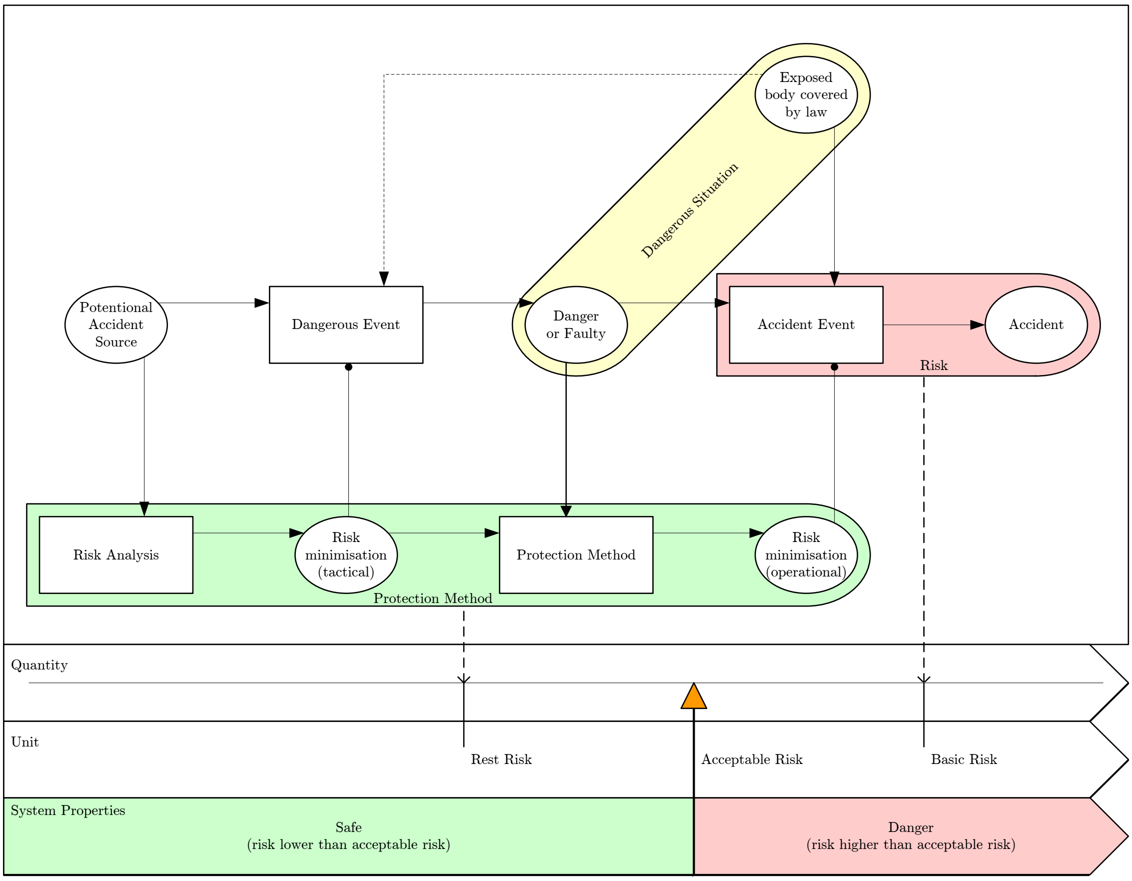


FIGURE 5.7: From Risk to Accident [87]

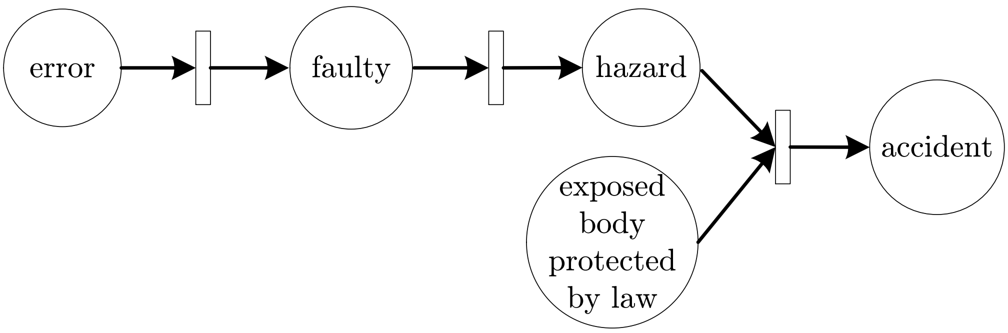


FIGURE 5.8: From Error to Accident

5.3 Migration of GNSS Performance Properties to Railway

The GNSS performance properties have been concluded as accuracy, continuity, availability, and integrity in Section 5.1. The railway quality of service has been introduced as reliability, availability, maintainability, and safety in Section 5.2. The relation between the two kinds of properties needs to be analysed, and then the gap

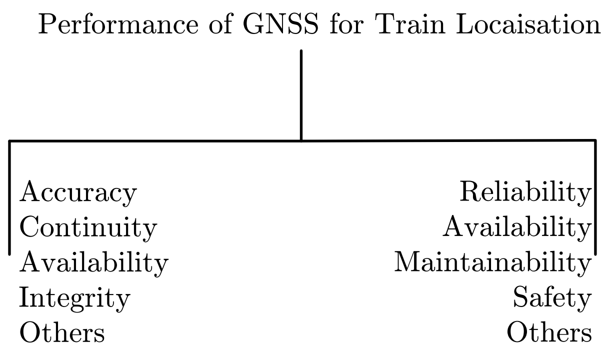


FIGURE 5.9: Performance Properties of GNSS for Train Localisation

between the two kinds of properties will be bridged. That is the migration process of GNSS for train localisation performance properties.

5.3.1 Relation between GNSS Performance and RAMS in General

The performance of GNSS for train localisation can be treated as the combination of both GNSS and RAMS performance properties. So the structure of the quality of service shown in Figure 5.2 can be redrawn as Figure 5.9. As seen directly from the figure, the common property of both is only availability.

According to the relation between GNSS performance properties, accuracy is the foundation of all other three properties. The continuity and reliability are having ambiguity between each other, both need to be compared in detail and then find the right one to be used in GNSS for train localisation. Then both integrity and safety are showing the information of "trust". The characteristic of integrity can be expressed through integrity risk, the characteristic of safety can be expressed through tolerable hazard rate. So both characteristics can be expressed by rate, that is the common characteristic for both. Besides, the maintainability from RAMS cannot find the corresponding property from the GNSS performance. Since the GNSS receiver or GNSS-based localisation unit are standing at the user segment, the GNSS SIS cannot be maintained by the user.

The relation between the GNSS QoS and railway signalling QoS is shown in Figure 5.10. The properties are listed with the consideration of equivalence, or to be more exactly the consideration of possible migration process.

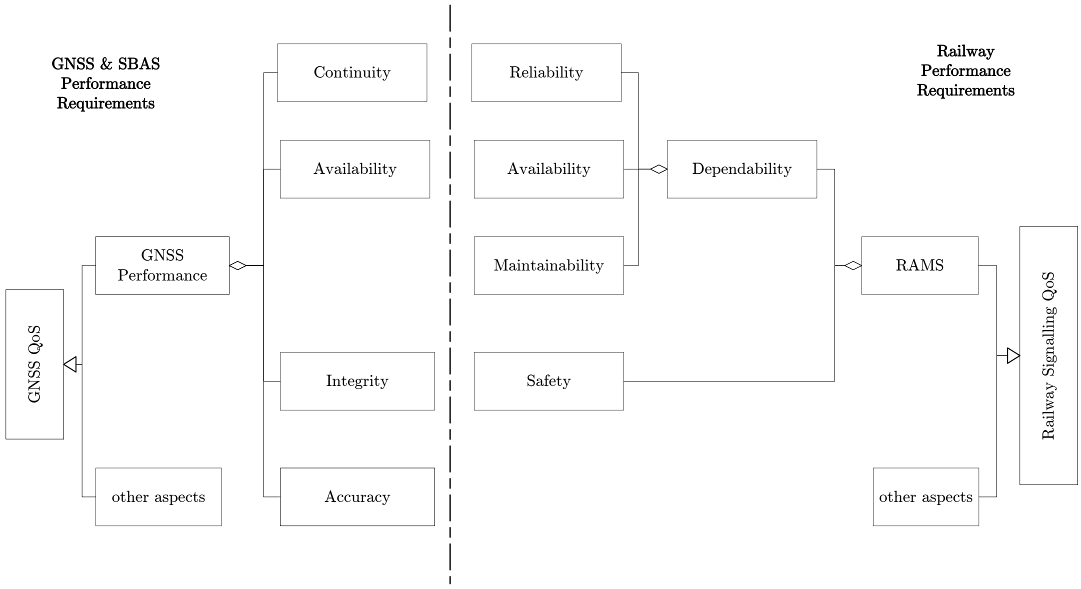


FIGURE 5.10: Relation between GNSS and Railway Signalling QoS Properties

5.3.2 Reliability and Continuity Migration

As already explained in Figure 5.3, failure rate is one of the characteristics for reliability, which is normally illustrated by λ if it is a constant. With the concept of failure analysis and optimal detection theory introduced in Chapter 3, the difference between reliability and continuity can be compared.

In the FRP document introduced in Chapter 4 Section 4.5, reliability (Definition 4.9) and continuity (Definition 4.8) are defined similarly. And reliability definition (Definition 5.1) in railway RAMS is also similar to FRP reliability.

For reliability defined in FRP and RAMS, the only difference is that FRP calls for "defined performance limits" but RAMS does not mention that. The both reliability definitions can be decomposed by three elements as:

- perform a required function
- within defined performance limits (by FRP) and under given operation condition (by RAMS and FRP)
- for a specific period time or a given time interval

And the continuity definition by FRP can also be decomposed identically with the reliability definition into three elements as:

- perform a required function

- without interruption
- during the intended operation

The first element is the same. The third element shows the time requirement. Reliability is defined clearly under a specific time interval, but continuity is defined in a intended operation which also has a time constraint. The difference exists in the second element. The second element of reliability definition by FRP and RAMS is the given conditions or defined performance, that is specified by a requirement value. Using GNSS for train localisation, the given operation condition can be the accuracy levels. The performance limit is also defined according to accuracy levels. But continuity only calls for without interruption, no requirement value is needed.

Considering the quantitative attributes for detection results shown in Chapter 3, the detected failures causes interruption to the system, that affects the continuity performance. But all the failures are outside the performance limit that affects the reliability performance. So continuity is related to detected failures $\lambda_{SD} + \lambda_{DD}$, but reliability is related to all the failures λ_{all}. In that $\lambda_{all} = \lambda_{SU} + \lambda_{SD} + \lambda_{DU} + \lambda_{DD}$.

So continuity can be understood as:

$$C(t) = e^{-(\lambda_{DD}+\lambda_{SD})t} \tag{5.4}$$

And reliability can be understood as:

$$R(t) = e^{-\lambda_{all}t} \tag{5.5}$$

Based on the mathematical expression, reliability is part of continuity as:

$$R(t) = C(t) \times e^{-(\lambda_{SU}+\lambda_{DU})t} \tag{5.6}$$

in that, $e^{-(\lambda_{SU}+\lambda_{DU})t} < 1$.

Based on the definitions and mathematical representations above, the relation between continuity and reliability can be expressed in Figure 5.11. The initially mixed up properties of "continuity" and "reliability" are now clearly distinguished through definition relation between the terms and attribute hierarchy representation of them.

The difference between continuity and reliability has also been analysed in other ways by Venn diagrams in [68]. That result reaches the same conclusion as stated above.

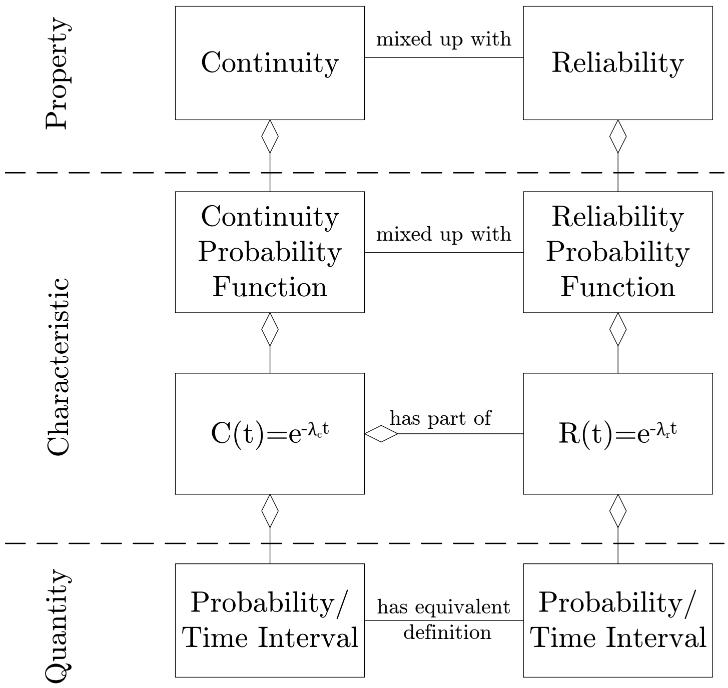


FIGURE 5.11: Relation between Continuity and Reliability in Attribute Hierarchy

GNSS for train localisation is a safety-related application, both the detected failures and the undetected failures need to be considered. Then reliability answers this call. So reliability is migrated as the property of GNSS for train localisation instead of continuity.

With the evaluation of the GNSS receiver locations, all the failures can be identified, thus λ_{all} can be estimated in Chapter 6. Reliability can also be estimated by $MTTF$ since $MTTF = 1/\lambda_{all}$.

5.3.3 Integrity and Safety Migration

The GNSS receiver location integrity is required by GNSS performance. Safety is generally required by RAMS. Both properties are extended by several characteristics. GNSS performance integrity is stated by four characteristics: integrity risk, alarm limit, time to alarm, and protection limit. But RAMS safety is stated by tolerable hazard rate in the requirements. Among the four characteristics of GNSS receiver integrity performance property, the "integrity risk" is related to RAMS "tolerable hazard rate".

Both characteristics are described by rates in a certain time interval. It is easy to mix up both characteristics when using GNSS for train localisation. As seen in

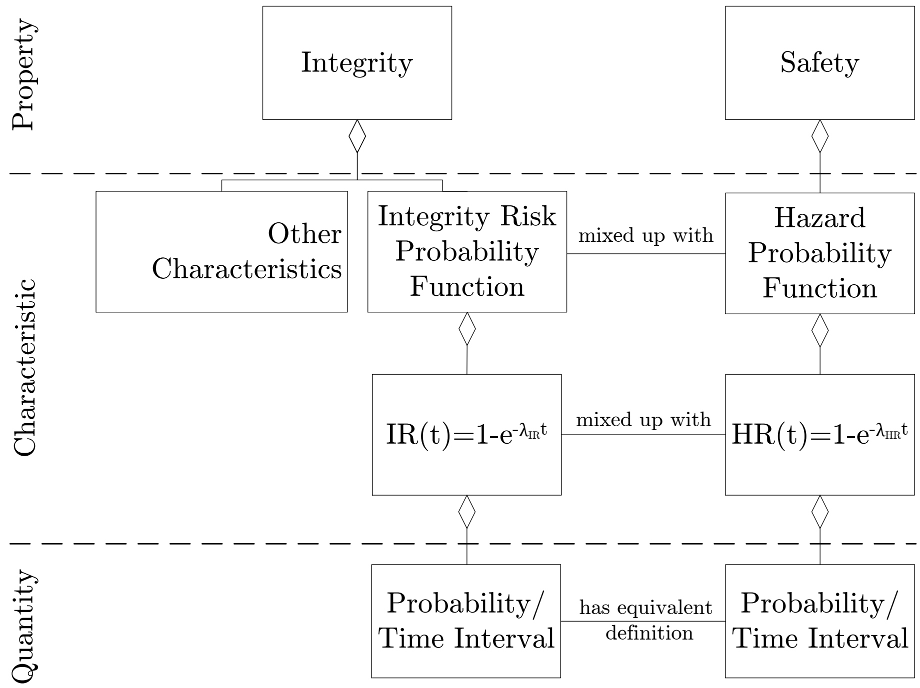


FIGURE 5.12: Relation between Integrity and Safety in Attribute Hierarchy

Figure 5.12, the difference between the both in the equations is only the λ_{IR} and λ_{HR}.

In GNSS receiver performance, the λ_{IR} is estimated according to the threshold of accuracy. The integrity risk can be understood as the accuracy level is beyond the alarm limit, but still no alarm is provided. This is according to the failure analysis part as $\lambda_{IR} = \lambda_{DU}$.

In RAMS, The hazard rate λ_{HR} is related to a dangerous situation of the system, that is the failure not detected in operation. That is also according to failure analysis as $\lambda_{IR} = \lambda_{DU}$.

So the $\lambda_{IR} = \lambda_{HR} = \lambda_{DU}$ in the context of GNSS for train localisation application. The integrity risk and hazard rate shows the same characteristic of GNSS for train localisation. The word “hazard rate” is chosen, because it states more clearly as a rate.

Now going up to the property level, both properties of “integrity” and “safety”, a new combined term is introduced as “safety integrity”. Safety integrity is the summary of all the related characteristics: hazard rate, alarm limit, time to alarm, as well as protection limit. But for train localisation, the safety margin is more commonly used than protection limit. So the safety margin is adopted instead of protection limit. As a summary, the safety integrity in this dissertation is stated by four characteristics:

- hazard rate: the hazard rate is considering the dangerous failures from the GNSS for train localisation function;
- alarm limit: the maximum allowable error in the measured location before an alarm is triggered;
- time to alarm: the maximum allowable time between an alarm condition occurring and the alarm being present at the output;
- safety margin: the margin for the safe distance between two trains.

5.3.4 GNSS for Train Localisation Properties Summary

Based on the migration process above, the common and applicable properties of GNSS for train localisation can be established. Since accuracy is the foundation of all other GNSS receiver performance properties, then accuracy is still a necessary property of GNSS for train localisation. Continuity has been migrated to reliability in the section above. Availability definition for GNSS and railway can be treated as the same, stated by stationary availability as A in a percentage function. Maintainability is not considered in this dissertation as already stated in Section 5.2. And the integrity, safety have been migrated to safety integrity which includes four characteristics. The comparison of the properties in Figure 5.10 can be migrated as shown in Figure 5.13 still having four properties. Then for the four properties, the characteristics and the quantities are shown in Figure 5.14.

With the established attribute hierarchy, the evaluation and verification methodologies and processes in the following Chapter 6 and Chapter 7 are basically based on the performance properties and characteristics in the attribute hierarchy structure in Figure 5.14.

5.4 Quantitative Requirements of GNSS for Train Localisation

The GNSS for train localisation performances need to be identified according to a settled quantitative requirements. This is also required by the system lifecycle V

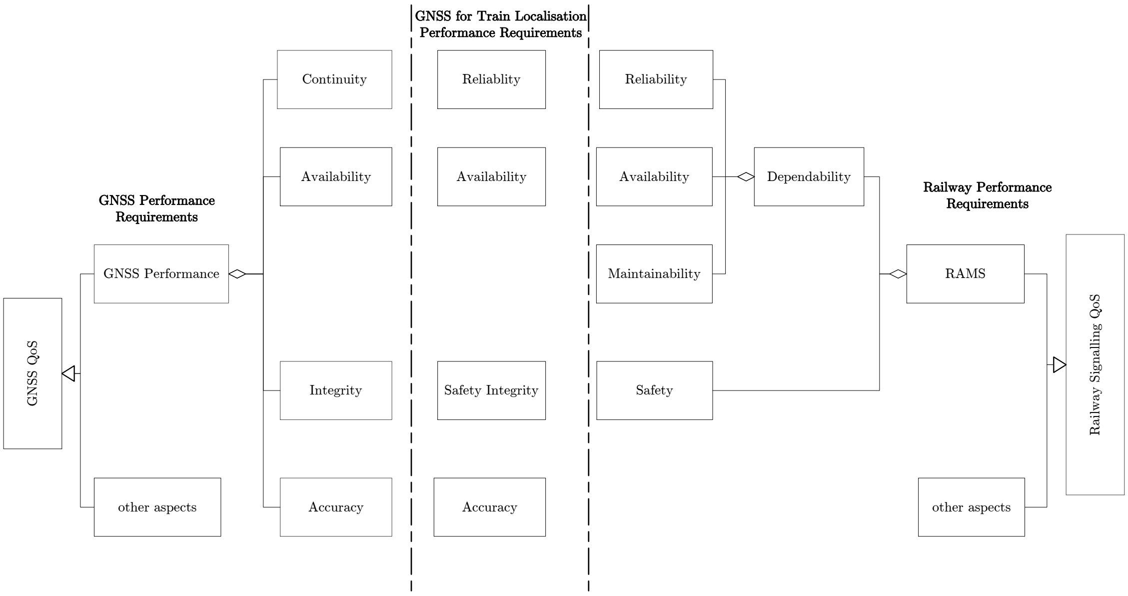


FIGURE 5.13: GNSS for Train Localisation Requirements

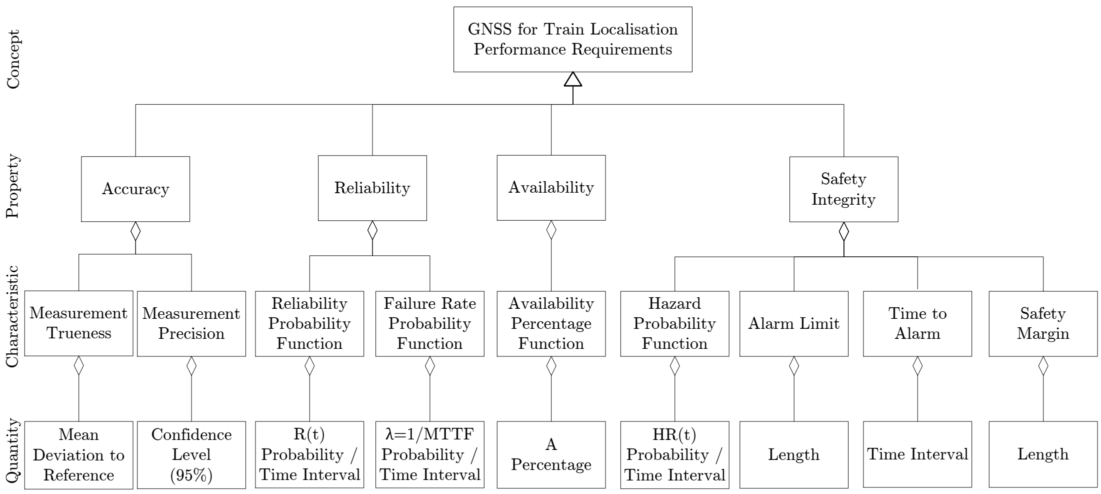


FIGURE 5.14: GNSS for Train Localisation Attribute Hierarchy

model in EN 50129 [20]. Using the established properties and characteristics, the values should be proposed.

The quantitative requirements can be mostly inherited from the GNSS for railway application performance advisories. In the evaluation part in Chapter 6, the test track can be regarded as a medium density line. Among the quantitative advisories, the hazard rate is not mentioned. So a value for hazard rate needs to be formally calculated from the existing aviation application performance value.

5.4.1 Quantitative Formalisation of Hazard Rate

As stated in the property migration part, the hazard rate of GNSS for train localisation is actually the dangerous undetected failure as λ_{DU}. According to the hazard rate in ICAO APV-I, it is stated as 2×10^{-7}/ 150 seconds. The chosen unit comes to 150 seconds, it is not the unit of the tolerable hazard rate in one hour time unit According to the difference in unit, a statement is describing the 150 seconds time interval as specific risk, and the one hour time interval as average risk [66]. The specific risk and average risk is defined as below:

Definition 5.15 Specific Risk (from [66])
Specific risk is the probability of unsafe conditions subject to the assumption that all credible unknown events that could be known occur with a probability of one (on individual basis).

Definition 5.16 Average Risk (from [66])
Average risk is the probability of unsafe conditions based upon the convolved (averaged) estimated probabilities of all unknown events.

In order to calculate the average risk from the specific risk, a stochastic Petri net model showing the process of the hazard is built in Figure 5.15. The one hour average risk contains 24 rounds of 150 seconds specific risk. Each "up state" is experiencing the 150 seconds time delay, and it is also possible to enter the hazard state with the negative exponential distribution with the value of 2×10^{-7}/ 150 seconds. After a fulfilment of the 24 up state periods, it survivals without a dangerous undetected failure. Thus the hazard rate in the unit of one hour can be formally calculated.

With the Monte Carlo simulation of the stochastic Petri net, the formalised result of the hazard rate in one hour time interval is estimated as 4.77×10^{-6}/ $hour$[12]. More details about this result can be found in a paper written by the author [141].

5.4.2 Proposed Values of GNSS for Train Localisation Performance

The migration process proposes the properties, the value of hazard rate as the characteristic for safety integrity is formalised to the one hour time interval. So the values of GNSS for train localisation performance on a medium density line can be proposed.

[12]This result is estimated from Monte Carol simulation.

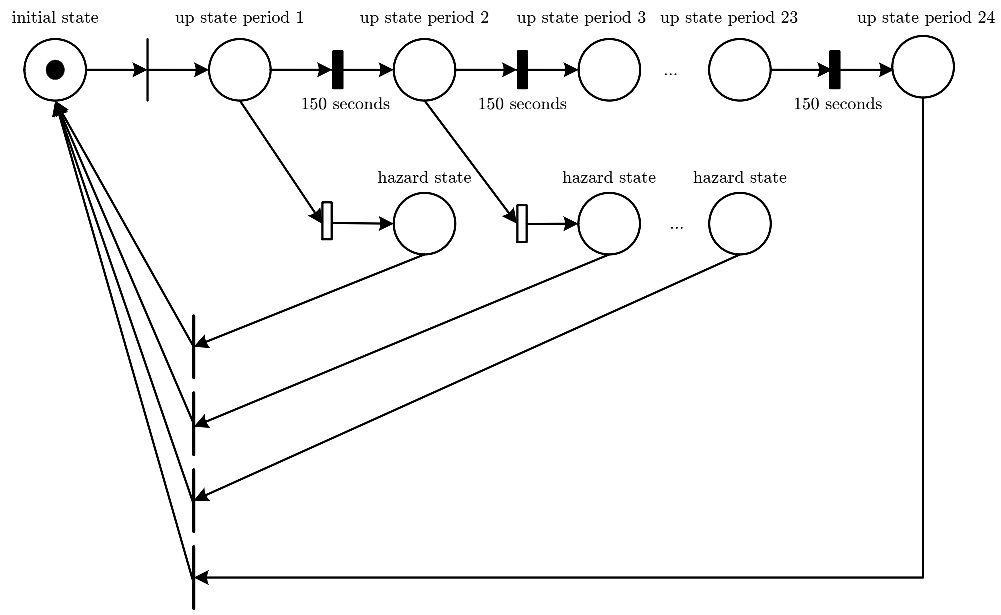


FIGURE 5.15: Integrity Risk Migration in Petri net Model

The accuracy, availability properties can both use the railway advisory values for the medium density line. The proposed reliability is related to continuity stated in the railway advisory, it can be inherited from that too.

The continuity of GNSS for railway medium density line is proposed as 99.98%/ hour, so

$$\lambda_{all} < (1 - 99.98\%)/\ hour$$

that is:

$$\lambda_{all} < 2 \times 10^{-4}/\ hour$$

The values of the four properties and the corresponding characteristics can be expressed in Table 5.5.

5.5 Chapter Summary

This chapter analyses the relation between the GNSS performance from the service provider side and the user side, the common properties of them are summarised as accuracy, continuity, availability, and integrity. The relation between the four properties are analysed, the accuracy is as the foundation of the other three properties.

Table 5.5: GNSS for Train Localisation Performance Requirement on Medium Density Line

Properties	Characteristics	Value and Unit
Accuracy	95% confidence level	10 m
Reliability*	failure rate	$\lambda_{all} < 2 \times 10^{-4} / \; hour$
Availability*	percentage	99.98%
Safety Integrity	hazard rate	$\lambda_{DU} \leqslant 4.77 \times 10^{-6} / \; hour$
	alarm limit	20 m
	time to alarm	$\leqslant$ 1 sec
	safety margin	real-time calculated

** For reliability and availability analysis, HDOP > 6 should also be excluded.*

The railway RAMS as the performance properties is also illustrated to show the corresponding properties and the included characteristics. The same structure of the GNSS performance properties and railway RAMS showing in the attribute hierarchy helps to identify the differences of the properties. Then the migration process of the properties aiming at GNSS for train localisation is done.

The proposed properties are accuracy, reliability, availability, and safety integrity. The characteristics for each property are also analysed and proposed. Based on the properties and characteristics, the values of the requirements are proposed based on the GNSS for railway application advisories for a medium density line.

The migrated properties, characteristics, quantities, as well as the proposed values help to identify the evaluated performance of GNSS for train localisation in next chapter.

Chapter 6

GNSS Receiver for Train Localisation Performance Evaluation

Evaluation is to determine system property values using criteria proposed by a set of documents such as specifications or standards. The GNSS performance evaluation needs a real entity that is the GNSS receiver. This chapter shows the evaluation methodology and process for the GNSS receiver locations regarding the migrated properties.

6.1 Accuracy Evaluation as the Foundation

When a GNSS receiver is installed on the train, the GNSS receiver delivers train location at a settled frequency. As the train is moving along the track, the GNSS receiver delivers different train locations and velocities. That is the so called dynamic measurement.

In dynamic measurement, precision of the locations are not easy to evaluate, because precision is the relation between the measured location and the true position. For statistic measurements, the mean value of the measured locations can be regarded as the true position with the sufficient number of measurements (Sometimes the measurement result contains an offset because of the systematic error.). In order to evaluate a dynamic measurement, a reference measurement system is required. With the reference measurement system, each GNSS receiver location can be compared with the reference location logged at the same time. This dissertation only evaluates the trueness characteristic of the accuracy, since the proposed requirement already put a performance limit to the accuracy level. More information about the precision

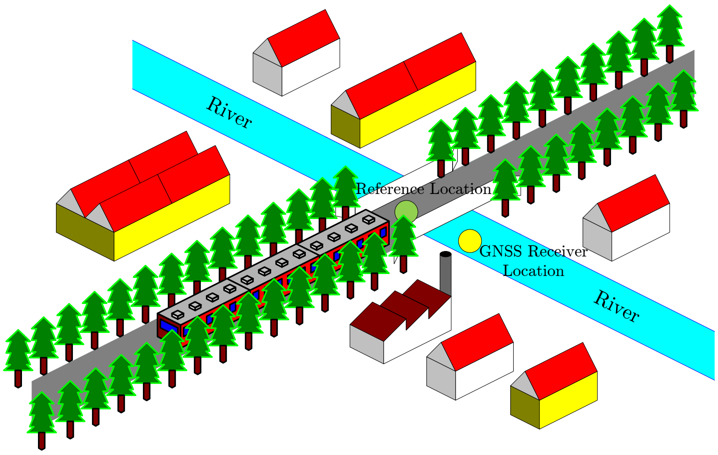


FIGURE 6.1: An Example of Measurement for GNSS Receiver Location and Reference Location

and measurement uncertainty have been investigated by Marco Wegener in the institute of traffic safety and automation engineering [142].

6.1.1 GNSS Receiver and Reference Locations

The GNSS receiver and the reference measurement system both deliver the train location. The two locations always have differences. In this dissertation it is called **deviation**. Figure 6.1 shows a train running on a track passing above a river. Because of the trees on the track side, the GNSS receiver location accuracy level is degraded. The GNSS receiver location indicates the train is outside of the track in the river, but the reference location shows that the train is on the bridge above the river. Definitely, the train should normally be on the track. The GNSS receiver locations need to be evaluated to see what is the accuracy level of the GNSS receiver, this requires a set of requirements to follow, and also a methodology.

Assume the GNSS receiver location to be given under Gauss-Krüger coordinate, and each GNSS receiver location at time t is recorded as $G_t = (x_{t,G},\ y_{t,G})$. The x means Gauss-Krüger Easting, and the y means Gauss-Krüger Northing. Each GNSS receiver location has its corresponding reference location at the same timestamp t named as $R_t = (x_{t,R},\ y_{t,R})$. The reference locations are all located on the track as shown in Figure 6.2 thanks to the digital track map as part of the reference measurement system.

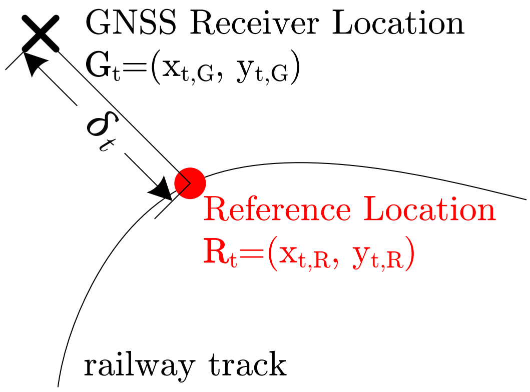


FIGURE 6.2: GNSS Receiver Location, Reference Location, and Deviation

The length of the vector $\overrightarrow{G_tR_t}$ is called deviation. The deviation is denoted as δ_t and it is calculated using Equation 6.1.

$$\begin{aligned} \delta_t &= |\overrightarrow{\mathbf{G}_t\mathbf{R}_t}| \\ &= \sqrt{(x_{t,G} - x_{t,R})^2 + (y_{t,G} - y_{t,R})^2} \end{aligned} \tag{6.1}$$

6.1.2 GNSS Receiver Location Accuracy Evaluation Process

The direct output of GNSS receiver location from the NMEA data is in WGS-84 coordinate. The components in the reference measurement system are delivering different measurements: the Doppler radar delivers velocity, the RFID sensor delivers the stored train location in Gauss-Krüger coordinate, the digital track map stores the POIs also in Gauss-Krüger coordinate. Finally the GNSS receiver location and the reference location are both converted into Gauss-Krüger coordinate. Then the deviation is calculated using Equation 6.1. The merit of the Gauss-Krüger coordinate is that it is a coordinate system in a plane, this makes distance calculation of two points easier than a sphere coordinate system. The whole process can be presented in Figure 6.3.

The deviation between GNSS receiver location and reference location indicates the accuracy level. The deviation can be illustrated in different ways. One way is to display the deviation as time series, the other way is to categorise the deviation into different levels, thus the probability density function of the measurements can be fitted to a certain probability model. As the understanding of the whole railway service, it can be regarded as a whole stochastic process [143]. The train localisation as part of the railway service is also a stochastic process. With the study of the time series and the probability model, the distribution of the accuracy level can be

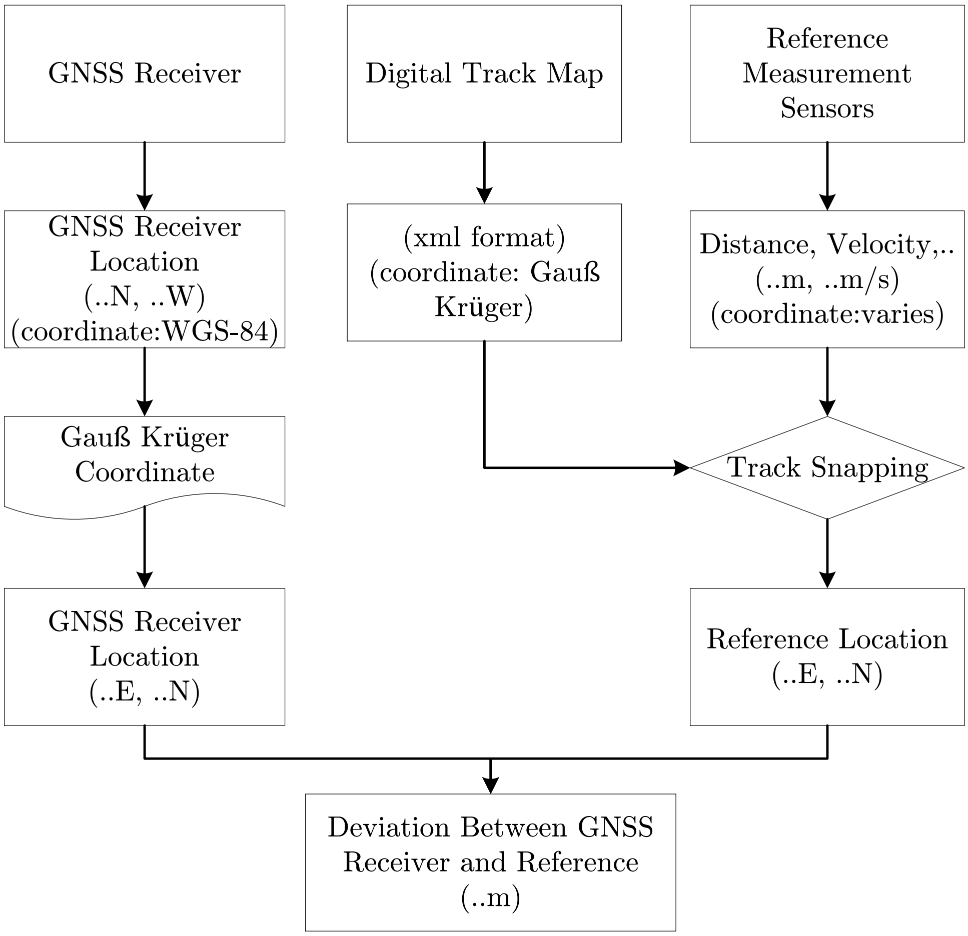


FIGURE 6.3: Accuracy Evaluation Process

determined, the process of the train localisation can be attributed to a certain kind of process.

6.2 GNSS Receiver Location Measurements Formalisation

The deviation value δ_t determines the accuracy of the GNSS receiver location.[13] For the evaluation methodology, the accuracy level needs to be identified. Thus a categorisation of the δ_t and the formalisation of it should be developed.

6.2.1 Assumptions

According to the real tests along the test track, the GNSS receiver is always powered on. So it is assumed that the GNSS receiver is running normally, systematic failures

[13]The accuracy of the reference system and the digital map is not the concern of this dissertation, so the deviation represents the accuracy level of the GNSS receiver.

are not included, only the random failures that affected by the signal reception environment are considered. The multipath and shadowing effect are the main affections.

The unique aspect about GNSS location measurements is that the GNSS receiver is delivering measurement results independent with each other, but they are affected by the same failure problem (e.g. bad satellite geometry). The GNSS receiver location accuracy varies in different scenarios related to the movement of the train. When the train is running on the railway track, it passes through different railway environmental scenarios (stated in Chapter 4). Then the strength of the signals, the mask angles of the satellites are changing over time and the place the train is. The GNSS receiver can deliver location measurements in one place (e.g. open area), and the GNSS receiver cannot deliver location measurements in another place (e.g. tunnel). This is from the system perspective regarded as self repairable. Besides, as stated before, the maintainability is not considered as the property of GNSS for train localisation.

The reference measurement system is considered to deliver accurate location at the timestamps compared with GNSS receiver location measurement. The performance of the reference measurement system will not be stated in this dissertation, it has been investigated by other colleagues in the institute [50] [89].

6.2.2 Formalise the Locations into States

As stated before, the system can be decomposed as having structure, function, state, and behaviour. Both structure and function have been introduced in Chapter 4, the state helps to identify the system performance level.

For example, the reliability tells the information about the faulty-free time intervals. The faulty-free is a state, the faulty is another. These states in the application of GNSS for train localisation are related to location measurements. So from the GNSS receiver perspective, three states are defined for the GNSS receiver locations. They are defined as follows:

- Up State: the GNSS receiver is powered up, the GNSS receiver location is reliable.
- Degraded State: the GNSS receiver is powered up, but the accuracy level of the location measurement is degraded, but still can be used for train localisation.

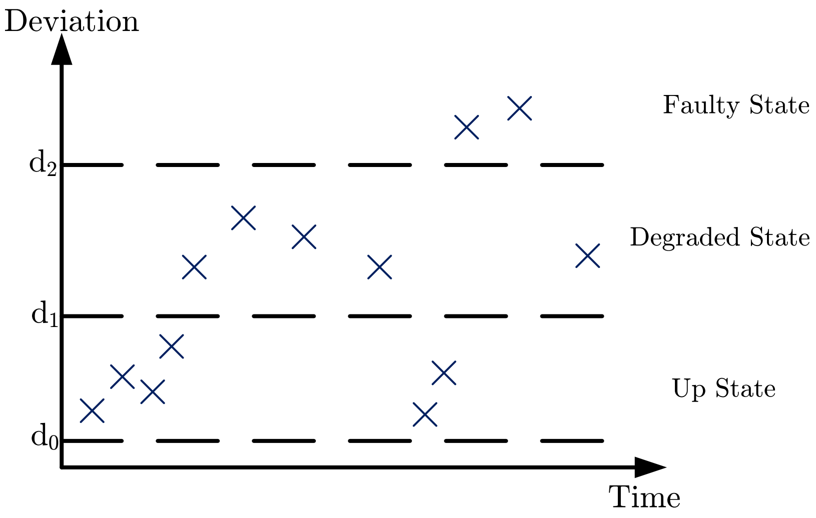


FIGURE 6.4: Relation between Defined States of GNSS Receiver Measurements

- Faulty State: the GNSS receiver is powered up, the measurement is unavailable due to GNSS signal loss or bad satellite geometry. Or when the GNSS receiver still delivers train location, but the accuracy level is beyond the performance limit, it is also a faulty state.

Remark 6.1 Faulty State Interpretation
Faulty state is the state that having failures. The undetected failures could cause hazards. According to the optimal detection theory introduced in Chapter 3, the faulty state can still be divided into four categories. The hazard happens when the failure is a dangerous undetected failure.

To identify the failures, the reference measurement system is used to determine the GNSS receiver location accuracy levels. Since each GNSS receiver location is accompanied with a reference location, each failure leading to the faulty state can be detected. So the undetected failures are assumed to be not existing in the evaluation process, that is to say the diagnostic coverage DC = 100%.[14]

All the definitions are based on the assumption that GNSS receiver is powered up. The accuracy level and the performance limit are both related to the deviation of the GNSS receiver locations stated as δ_t. The three states and the relation between the states and deviations can be shown very clearly in Figure 6.4.

When the deviation is lower than threshold d_1, then the GNSS receiver location is in the *Up State*. And, the deviation can also becomes bigger than d_1 but lower than another threshold called d_2, between the two thresholds the GNSS receiver location has higher deviation, but still under the performance limit, thus it is in the *Degraded*

[14]This number is stated as the total trust of the reference measurement system.

TABLE 6.1: GNSS for Train Localisation Deviation into States (Medium Density Line)

States	Value and Unit
up state	$\delta_t \leqslant 10$ m, and HDOP $\leqslant 6$
degraded state	10 m $< \delta_t \leqslant 20$ m, and HDOP $\leqslant 6$
faulty state	$\delta_t > 20$ m, or $\nexists\ \delta_t$, or HDOP > 6

State. Due to this degradation, GNSS receiver location may not be as reliable as the location in up state, but it still performs its required function, since it is under the performance limit. The third state is called *Faulty State*, which indicates it ceases to localisation function and is no longer available as a resource for the localisation function. The judgement criteria for faulty state also includes HDOP, the threshold for the maximum acceptable HDOP is dependent on the desired accuracy level [124].

6.2.3 Accuracy Formalisation

Accuracy is the foundation of all other three properties of GNSS for train localisation. The deviation is the basis for the accuracy evaluation. So the thresholds of deviations conclude the accuracy level.

When the δ_t is allocated in $d_1 < \delta_t < d_2$, the GNSS receiver locations are not accurate but still available for train localisation because of the performance limit is set as d_2. Referring the quantitative requirements of GNSS for train localisation raised for a railway medium density line after the migration process in Chapter 5 Table 5.5, the accuracy trueness characteristic is set as 10 m, the alarm limit characteristic for safety integrity is 20 m. So the up state threshold $d_1 = 10\ m$, and the degraded state threshold $d_2 = 20\ m$. The states and the deviations including the consideration of HDOP values can be shown in Table 6.1 as the basis for the deviation analysis of GNSS for train localisation on a medium density railway line. In that the HDOP value is set as 6, according to the normal HDOP acceptance defined in [22] and [133]. d_0 is the measurement uncertainty of the measurements.

Standing above a large number of GNSS receiver locations, a distribution fitting can be made either for all the data, or for one of the states. According to the distribution fitting theory introduced in Chapter 3 Section 3.4.3, the distribution of the deviation δ_t can be fitted to a symmetric distribution or non symmetric distribution. With the appropriate distribution allocated, the accuracy parameter μ and σ can be estimated.

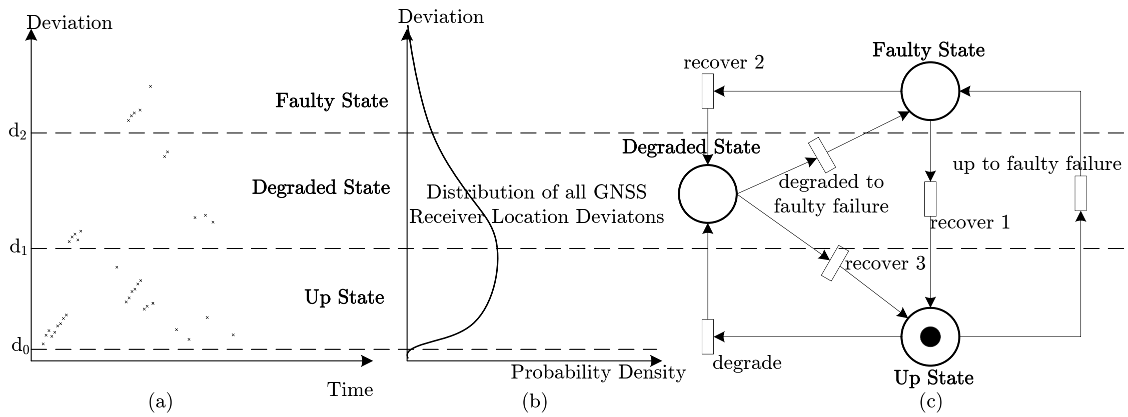


FIGURE 6.5: The Defined States, Distribution of the States, and the Petri net Model

A model based on stochastic Petri net showing the relation between the states according to standard IEC 62551 [144] [145] is established. The states for the Petri net model are the three states categorised in Figure 6.4. So Figure 6.5 (a) shows the GNSS receiver location deviations and the states again. Then in Figure 6.5 (b), the distribution of the whole GNSS receiver location measurement deviations is fitted as a distribution, and partially the up state alone is also fitted. After that, the transformation of the states through transitions is shown in Figure 6.5 (c).

The transition from up state to faulty state means the deviation of GNSS receiver location is already large enough, thus it is required for safety considerations and appropriate alarm notifications. The transition between faulty state and the other two states means both up state and degraded state can go to unavailable situations, and vice versa.

Comparing Figure 6.5 (a) and Figure 6.5 (c), the faulty state contains signal loss $\nexists\delta_t$ as safe failure; the faulty state also contains big deviation $\delta_t > d_2$ as dangerous failure. The big deviations are dangerous because without reference measurement system, the deviations are impossible to be quantified.

As assumed in Section 6.2.1, GNSS receiver locations are independent from the adjacent location. So the deviation going from one state to another is an independent event from the time series perspective. Normally process of the independent events is regarded as Poisson process, such as the events of arriving of the phone calls, the events of arriving of the customers to a shop, etc. [146]. The time between each event in a Poisson process assumed to follow the negative exponential distribution [146]. This leads to the reliability and availability evaluation.

6.2.4 Reliability and Availability Formalisation

Reliability and availability are two different properties of the same system. Reliability denotes the performance of the function, availability shows the result of the function performance. Reliability tells the information about the fail-free interval, and availability tells information about the percentage of failure-free in all the test results. So it is necessary to evaluate the reliability first, then the availability of the system performance can be derived from reliability performance.

The fail-free interval is the mean time to failure ($MTTF$) as one of the characteristics for reliability. So an individual fail-free interval is acknowledged as not in the faulty state time interval according to the state modelling. The individual **T**ime **t**o **F**ailure (TTF) can be defined as:

$$TTF_i = t_k - t_j + 1/f,\ \ k > j \tag{6.2}$$

In that, $\forall\ \delta_t,\ t \in (t_j, t_k)$ the δ_t follows $\delta_t \leqslant d_2$. f is the sampling rate of the GNSS receiver, the unit is Hz.

Besides, the deviation of measurement before time j (denoted as $\delta_{t(j-1)}$) and the measurement after time k (denoted as $\delta_{t(k+1)}$) obeys:

$$\begin{cases} \delta_{t(j-1)} > d_2 \quad or \nexists\ \delta_{t(j-1)} \\ \delta_{t(k+1)} > d_2 \quad or \nexists\ \delta_{t(k+1)} \end{cases}$$

So, all the individual fail-free intervals of TTF_i in the selected test are calculated as n, then the mean value of the TTF_i can be estimated by:

$$\begin{aligned} MTTF &= \frac{(samples\ of\ (up{+}degraded\ states))/(sampling\ rate)}{numbers\ of\ failure\ free\ interval} \\ &= \textstyle\sum_{i=1}^{n} TTF_i/n \end{aligned} \tag{6.3}$$

TTF_i and MTTF are all representing the time, that is recorded in this dissertation using second as the unit. So with the TTF_i, availability can also be calculated using it.

Availability is telling the percent of fail-free in all the tests. That is estimated by:

$$\begin{aligned} Availability &= \frac{samples\ of\ (up{+}degraded\ states)}{samples\ of\ (up{+}degraded{+}faulty\ states)} \\ &= \textstyle\sum_{i=1}^{n} TTF_i/T \end{aligned} \tag{6.4}$$

In Equation 6.4, T is the total test time.

6.2.5 Safety Integrity Formalisation

The safety integrity property contains four characteristics. The alarm limit, time to alarm are considered to be settled values. The safety margin needs to be real-time calculated, and it will be discussed in Chapter 7. The hazard rate needs to be formalised in this section.

The hazard occurs when the deviation $\delta_t > d_2$ or $\nexists\ \delta_t$ if it is not detected. $\delta_t > d_2$ means that the deviation is too large to be used for train localisation, so it is considered as a GNSS receiver location faulty state. $\nexists\ \delta_t$ means the deviation cannot be calculated, the cause could be signal loss, it is also a GNSS receiver location faulty state. With the reference measurement system, both faulty causes can be identified. Without the reference measurement system, only the $\nexists\ \delta_t$ can be identified. So $\nexists\ \delta_t$ is considered as a safe faulty state, and $\delta_t > d_2$ is considered as a dangerous state. For safety integrity analysis, the EN 50129 defines the unit of hazard rate as per hour per function. The function is the train localisation, the hazard is the $\delta_t > d_2$ when it is not detected.

As stated earlier, evaluation with the reference measurement system makes the DC=100%. So there are no problems with the undetected failures causing hazards. The evaluation can divide the failures into safe failures and dangerous failures. So rather than the hazard rate, the dangerous failure rate can be formalised and then evaluated. In the evaluation process, when $\delta_t > d_2$, it can be detected and collected.

Besides, the GNSS receiver location performance varies in different environmental scenarios as introduced in Chapter 4. So the dangerous failures needs to be analysed individually in different environmental scenarios.

The dangerous failures are collected, and then the dangerous failure rate λ_D per hour per train localisation function in a environment is estimated as:

$$\lambda_D = \frac{dangerous\ failure\ numbers\ per\ environment}{(samples\ per\ environment)/(sampling\ rate)} \tag{6.5}$$

In order to analyse the dangerous failure rate in each environment, the starting point POI_S and ending point POI_E of the environment in the digital track map needs to be identified beforehand. Assume there are n times of tests in this specific environment, the nearest GNSS receiver location to POI_S is $G_{t=t(S)}$ and the nearest GNSS receiver location to POI_E is $G_{t=t(E)}$. The measurement time for this specific

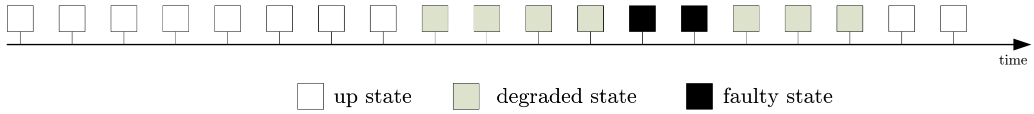


FIGURE 6.6: Measurement Series

environment in the i test is

$$T_{i,specific\ environment} = |t(E) - t(S) + 1/f|$$

, f is still the sampling rate of the GNSS receiver.

The dangerous failure number is counted when $(\delta_t > d_2) \cap (\delta_{t-1} \leqslant d_2)$, so the dangerous failure rate with m times of test in the specific environment is formalised as:

$$\lambda_D = \frac{\sum_{i=1}^{m} \sum_{t=min(t(S),t(E))}^{max(t(S),t(E))} (\delta_t > d_2) \cap (\delta_{t-1} \leqslant d_2)}{\sum_{i=1}^{m} T_{i,\ specific\ environment}} \tag{6.6}$$

The hazard in the dangerous failures are those who are not detected. The hazard rate of big deviation is calculated as $\lambda_{DU} = \lambda_{all} \times (1 - DC)$. But in the evaluation process, the DC is considered as 100%. So in the evaluation of the GNSS receiver location performance, only the λ_D is issued. The λ_{DU} is discussed and calculated in the GNSS for train localisation real-time verification part in Chapter 7.

6.3 Performance Evaluation Process

This section provides the evaluation process based on the formalised characteristics for each property in Section 6.2.

6.3.1 Reliability Evaluation Process

The reliability evaluation is based on deviations as shown in Equation 6.3. In the stochastic Petri net model of Figure 6.5, reliability is represented by both up state and degraded state. The criteria for reliability consists of two parts:

- There are GNSS receiver locations at the expected time t and $\delta_t < 20$ m;
- The HDOP value is acceptable. (HDOP $\leqslant 6$ according to [22])

The transition of the measurement data can be interpreted in Figure 6.6. From the data viewpoint, the measurements are just samples. To represent the reliability property, a **sample-based evaluation process** is proposed.

The algorithm for calculating $MTTF$ is as follows:

INPUT - NMEA data: GNSS receiver location, GNSS receiver location time, HDOP, number of visible satellites
INPUT - reference location, reference location time
OUTPUT - MTTF

---

1 Synchronise the same timestamp of reference location and GNSS receiver location.
2 Calculate the deviation between GNSS receiver location and reference location.
2.1 When timestamps of GNSS receiver locations are missing, mark a zero sign. It means a “faulty state” measurement.
2.2 When the deviation $\delta_t > d_2$, mark a zero sign. It also means a “faulty state” measurement.
2.3 When the HDOP > 6, mark a zero sign. It means a “faulty state” measurement.
2.4 When there are timestamps reference is missing, ignore the current timestamp.
3 Count each sample time span when there starts and ends with zero signs.
4 Count the numbers of the time spans in TTF_i.
5 Calculate the mean value of the time spans according to Equation 6.3, this represents MTTF of a test.

Now, the $MTTF$ is calculated through the mean value of the time to failures in one test, so each time is counted and categorised into the corresponding time span. Meanwhile, all the TTF_i are also stored. Then the possible distribution of the transitions in the Petri net model can also be estimated for simulation purpose. The calculation process can be shown as the following algorithm.

INPUT - NMEA data: GNSS receiver location, GNSS receiver location time, HDOP, number of visible satellites
INPUT - reference location, reference location time
OUTPUT - distribution fitting function, distribution parameter

---

1 Same as MTTF evaluation 1.
2 Same as MTTF evaluation 2.
3 Calculate the time span between two zero signs.

4 Count the number of the time spans n.
5 Categorise the time span into reasonable slots, using $\sqrt{n}$.
5.1 Categorise the time spans into slots till more easy fitted.
5.2 Using maximum likelihood method to find the best fitted distribution.
5.3 Estimate the parameter for the distribution, for example λ.

The distribution function and the parameter for the distribution function show the parameter for the transitions in the stochastic Petri net model.

6.3.2 Availability Evaluation Process

Availability of GNSS receiver locations is not the same as the availability of GNSS SIS. Availability of GNSS SIS means the percentage the system is usable with a good signal reception environment, but availability of GNSS receiver locations is the percentage of the locations that are acceptable for train localisation in a defined test run.

For example, the EGNOS availability is usually calculated in relation to the percentage of time when the protection levels (HPL and VPL) are below their threshold values (set for a type of operation by the alarm limits, i.e. HAL and VAL) [147]. This is the same as the defined up state and degraded state in this dissertation.

The principle and algorithm for estimating the availability is as follows:

INPUT - NMEA data: GNSS receiver location, GNSS receiver location time, HDOP, number of visible satellites
INPUT - reference location, reference location time
OUTPUT - stationary available percentage

---

1 Synchronise the same timestamp of GNSS receiver location and reference location.
2 Calculate the deviation between GNSS receiver location and reference location.
3 Count the total samples of the measurement time as T.
4 Count the samples when there are deviations without zero sign from the reliability evaluation process ($\sum TTF_i$).
5 Calculate the percentage of the two parameters in process 3 and 4 according to Equation 6.4.

The availability shows the general percentage of the GNSS receiver can be used for train localisation. The unavailability of the GNSS receiver locations affects the safety integrity performance, the evaluation process for dangerous failure rate as a characteristic for safety integrity is introduced in the next section.

6.3.3 Dangerous Failure Rate Evaluation Process

Similar to reliability and availability, safety integrity is also affected by the railway environmental scenarios. In order to show the dangerous failures with consideration of the environmental scenarios, the dangerous failure rate evaluation process is introduced as environmental scenarios related.

The following process is using one environmental scenario as an example. The starting point of the environment POI_S and the end point of the environment POI_E is interchangeable to other environmental scenarios. So the process of dangerous failure rate evaluation is as follows:

INPUT - NMEA data: GNSS receiver location, GNSS receiver location time, HDOP, number of visible satellites; environment begin POI POI_S; environment end POI POI_E
INPUT - reference location, reference location time
OUTPUT - λ_D

---

1 Synchronise the same timestamp to both GNSS receiver location and reference location.
2 Calculate the deviation between GNSS receiver location and reference location.
3 Identify the clip of the GNSS receiver location inside the environmental scenario POI_S and POI_E.
4 Calculate the time of this environmental scenario as T_i.
5 Calculate the dangerous failure number in this test run.
6 Calculate the number of dangerous failures in this test run.
7 Redo the process with n times of test in this environmental scenario.
8 Estimate the dangerous failure rate λ_D in this environmental scenario according to Equation 6.6.

The dangerous failure rate provides the understanding of safety issues of GNSS for train localisation even though it is normally bigger than the hazard rate.

With the formalised characteristics of the GNSS for train localisation performance properties and the evaluation process based on the formalised characteristics, the evaluation on the real data can be performed.

6.4 Setup of Evaluation Platform

In order to evaluate GNSS, an evaluation platform was built, and test scenarios are predefined. Between 2008 and 2009, the DemoOrt project was implemented in several test tracks [148]. The basic idea of DemoOrt is the set up of a vehicle side on-board platform, utilising and integrating innovative technologies, with a focus lying on satellite-based localisation (GNSS). The system is designed to be highly available and provides localisation information for applications especially for those with safety responsibility. To achieve these goals, a sensor data fusion on different sources of localisation information is implemented. This also gives diversity and redundancy of the localisation information, increasing the safety, accuracy, and availability of the whole system [149].

6.4.1 Test Area and Test Locomotive

The GNSS receiver location data along the High Tatra Mountains railway line was collected from May 2008 to February 2009 in different climate conditions and seasons.

The High Tatra Mountains railway line is called *Tatranská elektrická železnica* in Slovakia. It is an electrified single track narrow gauge railway in the Slovakia side of the High Tatra Mountains. The whole line is 29.1 km long from *Poprad-Tatry* to *Starý Smokovec* till *Štrbské Pleso.* There are open areas, and forests, as well as high altitude change along the line. The map of the High Tatra Mountains railway line is shown in Figure 6.7.

The altitude of the track varies from 600 m to 1400 m, it is plotted into Matlab as shown in Figure 6.8, the train used for the test is also illustrated in Figure 6.9.

6.4.2 Measurement Project Introduction

The DemoOrt platform consists of three parts: the GNSS receiver itself; the reference measurement system integrated by RFID sensors and antennas, Doppler radar

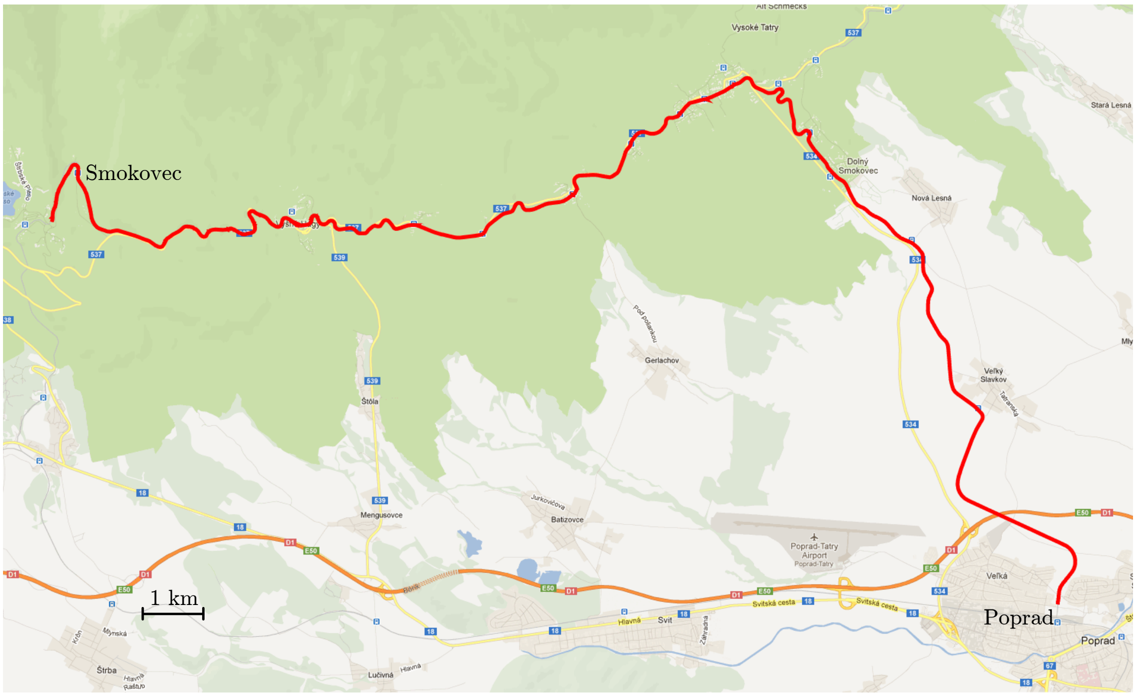


FIGURE 6.7: Map of High Tatra Mountains Railway Line

TABLE 6.2: Sensors for DemoOrt Platform

Sensor	Data Frequency	Function
GNSS Receiver	2 Hz	real-time train localisation
Doppler Radar	10 Hz	velocity measurement
RFID Sensor/Transponder	n.a.	detect transponders on the track
Digital Track Map	n.a.	reference for sensor fusion

and a digital track map; and the software data processing. The composition of DemoOrt platform is displayed in Figure 6.10. GNSS receiver, reference measurement system, and process control are marked in different grey level. The data frequencies and functions of each sensor in Figure 6.10 are listed in Table 6.2.

Including the hardware and sensors above, a software called *qDemoOrt* is developed, which is part of the software data processing. *qDemoOrt* processes all the information from the sensors except GNSS receiver. An electronic track map is used as a reference for sensor fusion, thus relating all the location data directly on the track. The fusion result of all the sensors is synchronised with GNSS receiver output all at same timestamps. The output frequency of *qDemoOrt* is the same as GNSS receiver, which is 2 Hz.

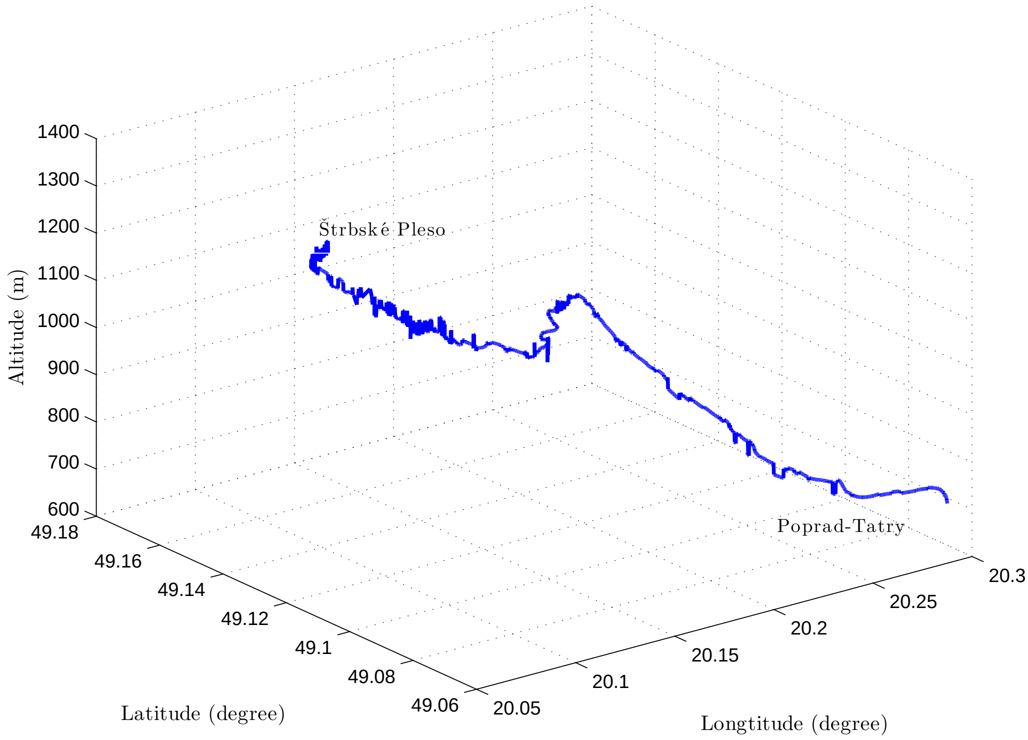


FIGURE 6.8: Altitude Changes of the High Tatra Mountains Railway Line

FIGURE 6.9: Test Train for High Tatra Mountains Railway Line

6.4.3 Reference Measurement Platform Composition

The setup of the reference measurement system is based on the idea of independent evaluation and identification of GNSS receiver localisation results. For approval or certification purposes of GNSS on railway train localisation applications, the

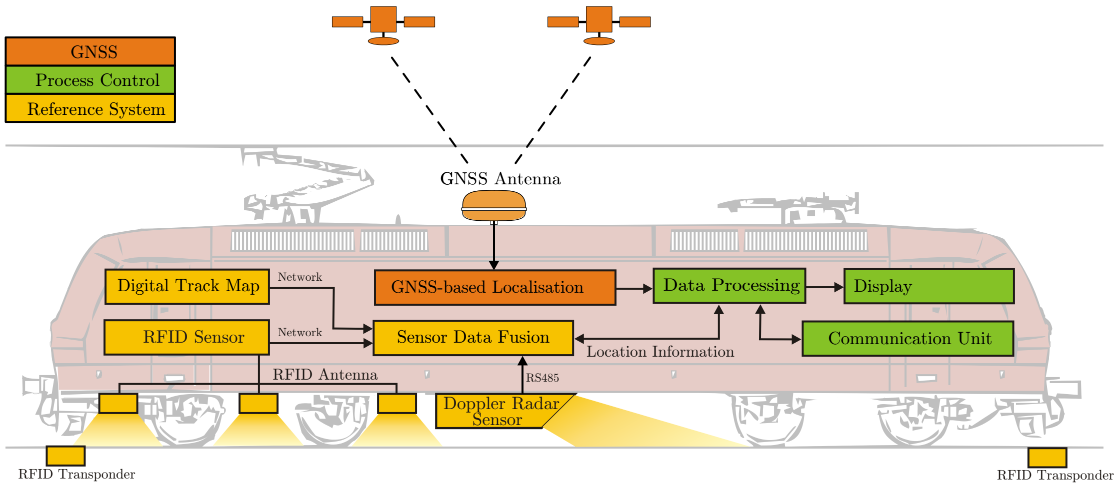


FIGURE 6.10: DemoOrt Structure

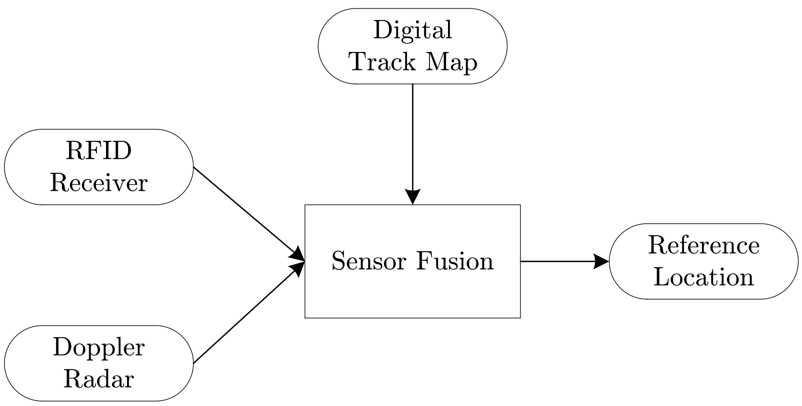


FIGURE 6.11: DemoOrt Reference Measurement System Structure (*qDemoOrt*)

basic proof of RAMS has to be enhanced by a safety case according to CENELEC standards [149].

The reference measurement system generates train reference location in real time. It performs almost the same functionality as a GNSS receiver but not related to GNSS or affected by GNSS at all. Besides, it is not environment sensitive, when the GNSS SIS is affected by the environment, the reference measurement system is still available. Since the output of the reference measurement system is compared with GNSS at the same timestamp, the deviation between GNSS and reference measurement system can be calculated for every location for all the test runs. The reference measurement system sensor outputs are all inputs for *qDemoOrt* sensor fusion process. The whole process is presented in Figure 6.11. The deviation between each GNSS receiver location and reference location is calculated for RAMS evaluation based on the accuracy evaluation process described in Chapter 6 Section 6.1.

6.5 Numerical Results of Performance Evaluation

The measurements along the track are collected for almost one year. So the evaluation process not only needs to consider the performance of each function, but also needs to consider the performance in different environments or in different seasons. According to the evaluation results, the season doesn't have large effect on the accuracy evaluation results.

6.5.1 GNSS Receiver Measurement General Statement

The GNSS for train localisation performance evaluation procedure is implemented according to the methodology proposed in this chapter before. The data is used to evaluate all the properties for the requirements described in Figure 5.13 (Chapter 4 Section 5.3) thoroughly. Double tracks only exist on four stations, so the line can be treated as a medium density line. According to the requirement stated in Chapter 5, the acceptable accuracy level should be lower than 10 m (95%), and alarm limit is 20 m.

According to the measurement setup of the train localisation, the GNSS receiver is installed on the locomotive as part of OBU, the GNSS receiver is always powered on. So the 24 hours measurements are logged. For the evaluation, only the test runs are considered, so it is necessary to omit the operations like shunting, standby for the night, etc. The measurements from the end station to the nearest station are ignored, which means the measurements from *Poprad-Tatry* to *Vel'ký Slavkov* and from *Štrbské Pleso* to *Popradské Pleso* are not considered, since there always exists systematic offsets in the two parts. And the data chosen to be evaluated is on 16 May 2008 and 3 February 2009.

6.5.2 Accuracy Evaluation

Accuracy evaluation is based on the deviation of the GNSS receiver locations in the test runs. According to the parameters settled in Chapter 5, the accuracy level is

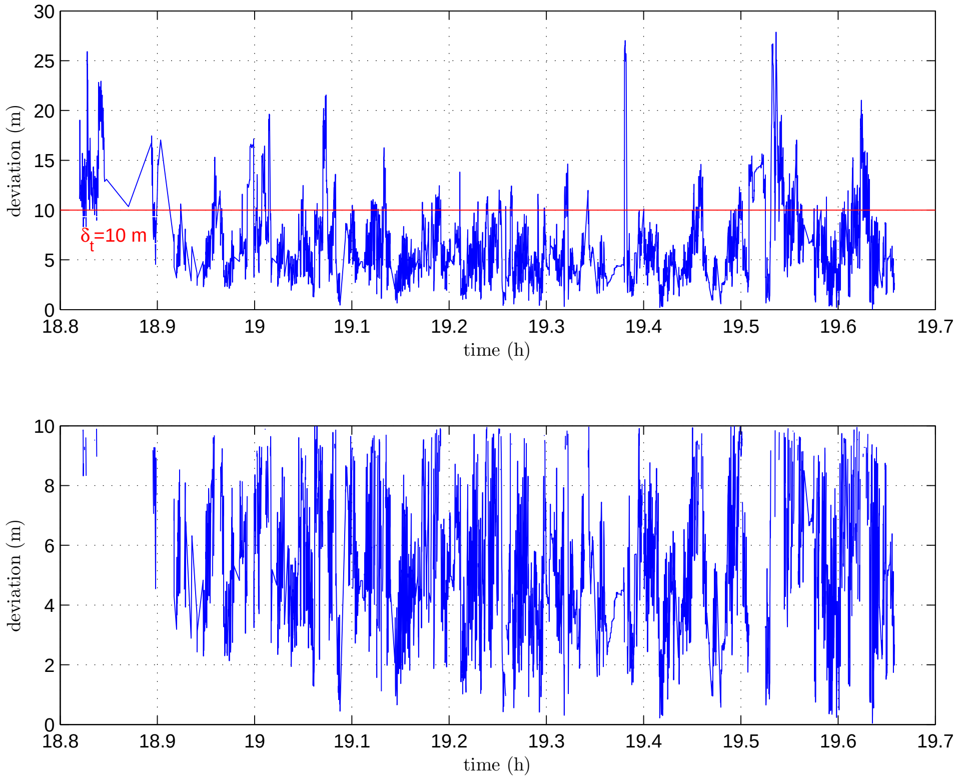


FIGURE 6.12: Deviation of One Test Run from *Popradské Pleso* to *Vel'ký Slavkov*

10 m ($d_1 = 10\ m$) which is considering 95% of all the deviations, the alarm limit is 20 m ($d_2 = 20\ m$). The parameters are considered for a medium density line.

On the whole day of GNSS receiver locations on 16 May 2008, there are four complete test runs. Two test runs are from *Štrbské Pleso* to *Štrbské Pleso*, the other two are the way back. The deviation of the fourth test run from *Popradské Pleso* to *Vel'ký Slavkov* is shown in Figure 6.12.

In Figure 6.12, the biggest deviation reaches 27.86 m, this deviation has already exceeds the alarm limit. The percentage of the data that is under accuracy level 10 m is only 82.48%. The deviations are fitted into possible distributions as shown in Figure 6.13. The deviations are calculated and then fitted into the possible distributions (Rayleigh distribution and Log-normal distribution). The Log-normal distribution and Rayleigh distribution are both left skewed (negative skew), according to the significance of the two distribution fitting results, the Log-normal distribution fits better than Rayleigh distribution.

Since the deviation between the GNSS receiver location and reference measurement location and the GNSS location is actually represented by two axises. The deviation

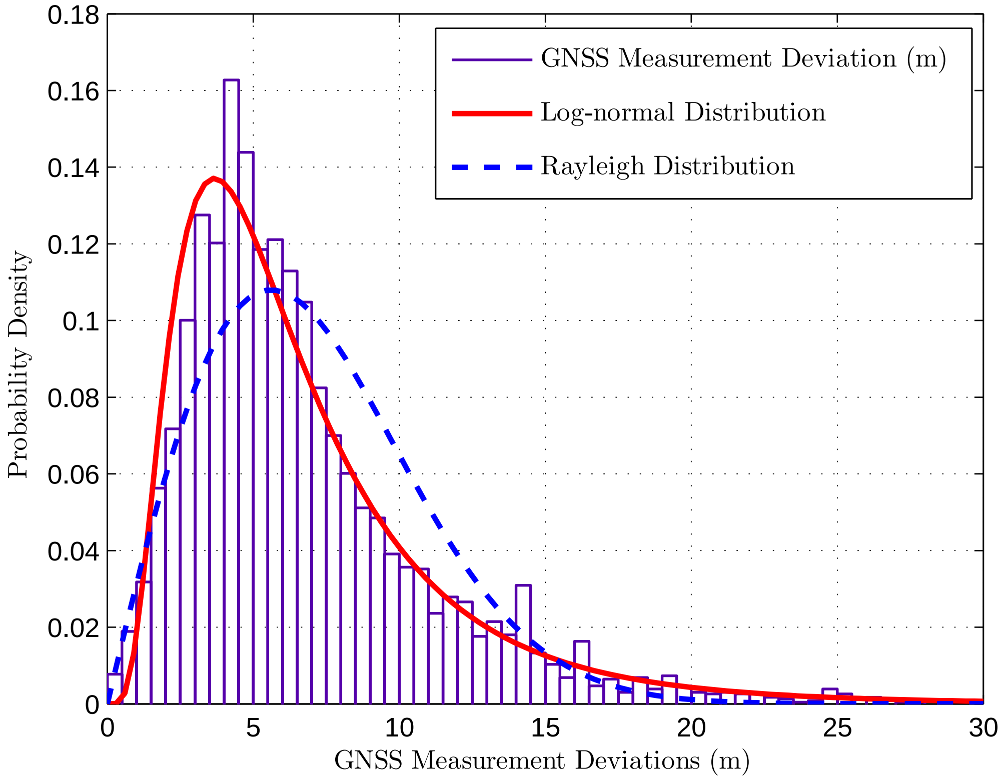


FIGURE 6.13: δ_t Fitting of One Test Run

calculation is generated by RSS. When the $\mu_x = \mu_y = 0$ and $\sigma_x = \sigma_y = \sigma$, the RSS follows Rayleigh distribution. And when the $\mu_x >> \sigma_x$ and $\mu_y >> \sigma_y$, then the RSS follows normal distribution. In other situations, the RSS follows Log-normal distribution. According to the deviation measurements of the DemoOrt project, the jitter of the messages from the GNSS receiver and reference measurement system gives measurement uncertainty of the deviations. Besides, the accuracy level of the reference measurement system also provides uncertainty of the measurements. For example, in Figure 6.12 the deviation never reaches 0, which means a measurement uncertainty with d_0 exists in the measurements.

Since the measurement uncertainty is not the concern of this dissertation, the following sections and chapters will live on the accuracy level of the reference measurement system and generate the quantitative values based on that. For the Log-normal distribution of the deviations, the parameters for Log-normal distribution are also μ and σ. In order to be identical with the requirements of the 95% of the deviations, the deviation limit for the 95% is also applied. The percentage of the 10 m accuracy level is also calculated for comparing the two percentage values. The parameters of the four test runs on 16 May 2008 is shown in Table 6.3.

TABLE 6.3: Deviation Log-normal Distribution Fitting Parameter on 16 May 2008

parameter	test run a1	test run a2	test run a3	test run a4
μ (m)	6.02	6.31	5.57	6.84
σ (m)	29.71	14.13	27.51	24.11
δ_t 95% (m)	16.48	13.81	14.74	14.98
10 m percentage	89.50%	88.41%	90.49%	82.48%

TABLE 6.4: Deviation Log-normal Distribution Fitting on 3 February 2009

δ_t	test run b1	test run b2
μ (m)	4.02	8.69
σ (m)	10.07	52.73
δ_t 95% (m)	10.67	12.31
10 m percentage	93.95%	87.6%

Besides the test runs on that day, other test runs are also evaluated. For example, the test run from *Vel'ký Slavkov* to *Popradské Pleso* on 3 February 2009 is also evaluated. The mean value and standard deviation for both test runs fitting in Log-normal distribution are shown in Table 6.4.

So when not considering the signal loss, only evaluating the available GNSS location measurements, the 95% of the measurements can be regarded as 13.83 m based on the six test runs shown above.

6.5.3 Reliability and Availability Evaluation

General reliability and availability evaluations are estimating the MTTF and MTTR then calculating the availability percentage. This has been illustrated in Chapter 6 Section 6.3. The examples to be shown are also on 16 May 2008 and 3 February 2009.

Like the accuracy evaluation, only the data collected during the movement of the train is used for reliability and availability evaluation. When considering the test runs on each day, the MTTF value is higher than the whole day.[15] The criteria for the reliability and availability are listed again:

- $\exists\ \delta_t$, and $\delta_t < 20$ m,

[15]Because the whole day consists the time train is in the area without any GNSS signal reception.

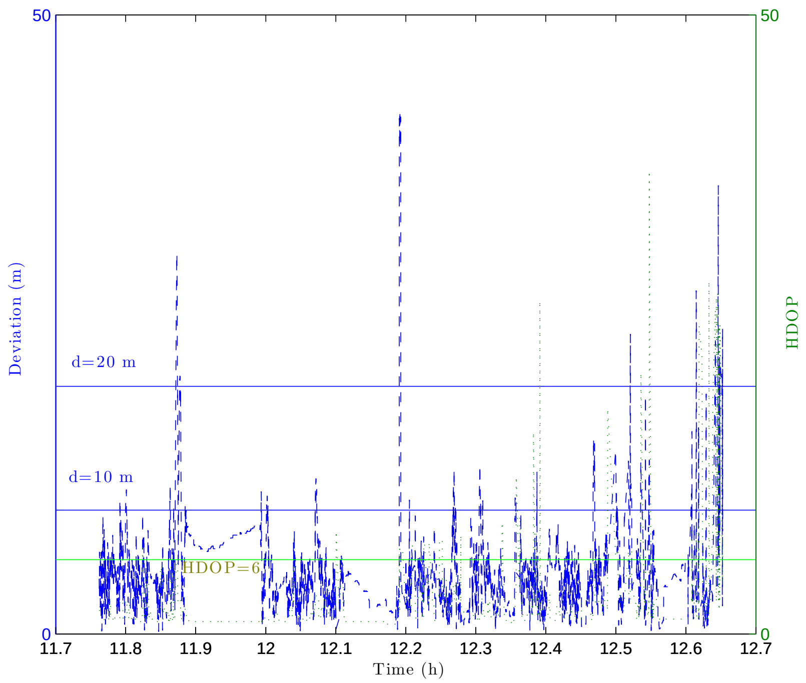


FIGURE 6.14: Deviation and HDOP thresholds for the first test run on 16 May 2008

- HDOP < 6.

Based on these two listed criterions, the reliability and availability analysis in each test run is evaluated. And the information of deviation, HDOP, and timestamp loss is shown in Figure 6.14.

With the evaluation of the six test runs on both days. The MTTF can be calculated through the failure numbers and total up and degraded states time. The availability of GNSS receiver measurements is also attributed to HDOP, number of visible satellites, deviation smaller than 20 m. So in the evaluation below, the availability of the first test run on 16 May 2008 is considered as:

- $\delta_t > d_2$ faulty state time: 111.5 seconds,
- $\nexists\ \delta_t$ faulty state time: 353.5 seconds,
- up and degraded states time: 2742 seconds.

So the availability is represented as

$$A = \frac{2742}{2742 + 111.5 + 353.5} = 85.50\%$$

Table 6.5: Reliability and Availability of Each Test Run on 16 May 2008

Test Sequence	test run a1	test run a2	test run a3	test run a4
MTTF (sec)	161.29	312.11	104.81	75.24
Availability	85.50%	80.30%	81.29%	72.31%

Table 6.6: Availability of Each Test Run on 3 February 2009

Test Sequence	test run b1	test run b2
MTTF (sec)	393.75	62.74
Availability	92.44%	81.69%

Each MTTF and available percentage for each test run on 16 May 2008 is shown in Table 6.5, accordingly the information about the test runs on 3 February 2009 is shown in Table 6.6.

So based on the six test runs, the MTTF for them all is:

$$\begin{aligned} MTTF &= 184.99 \; seconds \\ A &= 82.26\% \end{aligned}$$

6.5.4 Transition Distribution in the Stochastic Petri net Model

With the reliability and availability evaluation, the Petri net model proposed in Chapter 4 can be quantitatively modelled not only for the states but also for the transitions. The Petri net model is redrawn from Figure 6.5 (c) in Chapter 6 to Figure 6.15. In the model, the distribution of the six transitions can be fitted from the measured individual time span staying in one state to another.

The same six test runs in reliability and availability evaluation are analysed together to provide enough data for the transition firing time fitting. In this section, the parameter calculation method for MTTF is not applied for the transition firing time estimation, the distribution fitting is used to find the distribution of the firing time. The time to alarm is already defined as lower than 6 seconds (Chapter 5 Table 5.5), this is also taken into consideration for the transition fitting.

The time from up state to degraded state transition and the time from degraded state to up state transition time are both categorised in Figure 6.16. It shows that the time to the other state distribution can be regarded as negative exponential distribution for both transitions in a primary approximation. The other four transitions are also analysed and modelled as shown in Figure 6.17. The results show

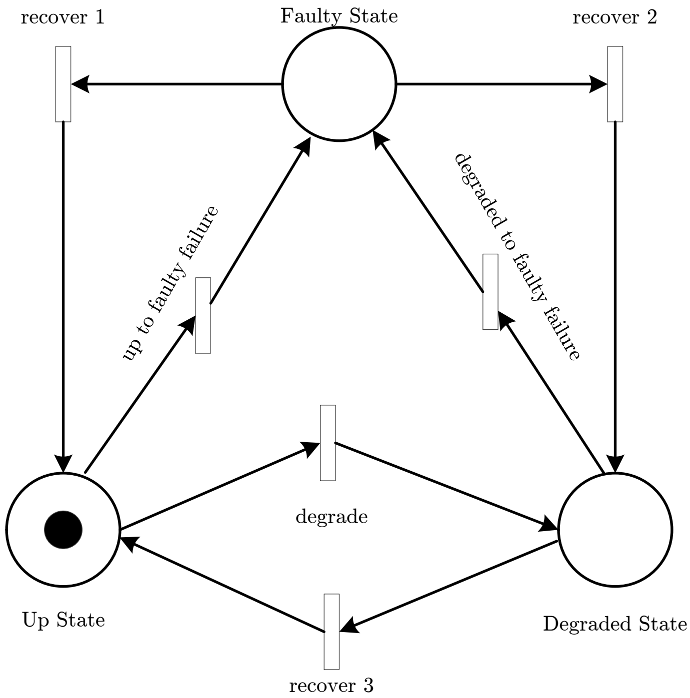


Figure 6.15: Petri net Model for States and Transitions

Table 6.7: Distribution of Each Transition and Parameter

Transition	mean time (sec)
up state to degraded state transition	15.31
degraded state to up state transition	2.46
up state to faulty state transition	20.79
faulty state to up state transition	5.91
degraded state to faulty state transition	2.88
faulty state to degraded state transition	6.71

that all six transitions can be fitted to negative exponential distributions. The mean value is calculated and rate is also estimated in Table 6.7.

Remark 6.2 Illustration of Negative Exponential Distribution
The transition from any of the three states are evaluated, the result shows that they all obey the negative exponential distribution. The negative exponential distribution is memoryless which represents the measurement series of GNSS receiver very well. Each dynamic measurement is independent with each other.

According to the evaluation result, the probability of staying in the up state is

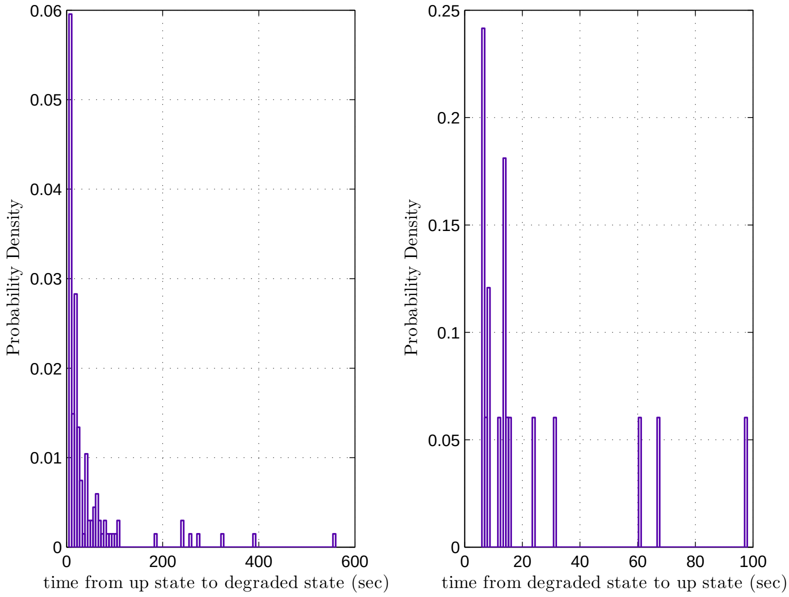


FIGURE 6.16: Time for the Two Transitions between *Up State* and *Degraded State*

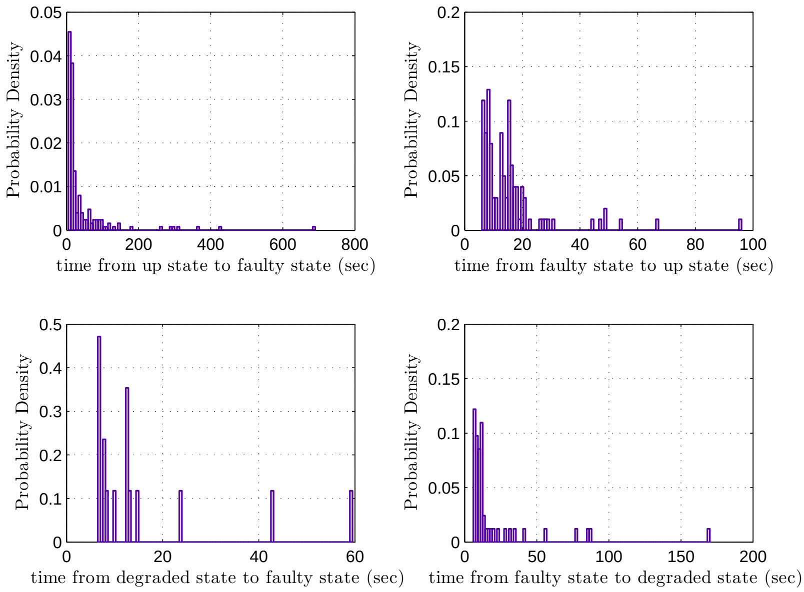


FIGURE 6.17: Time for the Rest Four Transitions between Three States

73.69%, staying in degraded state is 7.92% and staying in faulty state is 18.39%. Based on this, the parameter for the transitions are now simulated, this structure will be useful for the safety evaluation and further localisation unit evaluation.

Table 6.8: Time of Signal Loss in the Test Run

Test Sequence	Signal Loss (min)	Total Test Time (min)	Percentage
test run a1 (on 2008-05-16)	5.89	53.45	11.02%
test run a2 (on 2008-05-16)	10.84	58.30	18.60%
test run a3 (on 2008-05-16)	7.49	51.58	14.53%
test run a4 (on 2008-05-16)	11.48	50.29	22.83%
test run b1 (on 2009-02-03)	3.86	56.79	6.79%
test run b2 (on 2009-02-03)	6.19	60.17	10.29%

Table 6.9: Time of Deviation Bigger than 20 m

Test Sequence	Big Deviation (min)	Total Test Time (min)	Percentage
test run a1 (on 2008-05-16)	1.86	53.45	3.48%
test run a2 (on 2008-05-16)	0.64	58.30	1.10%
test run a3 (on 2008-05-16)	2.16	51.58	4.18%
test run a4 (on 2008-05-16)	2.44	50.29	4.86%
test run b1 (on 2009-02-03)	0.43	56.79	0.76%
test run b2 (on 2009-02-03)	4.83	60.17	8.02%

6.5.5 Safe Failures to the Faulty State

According to the evaluation in the last section, the faulty state is formed by 18.39%. In that, one part of the faulty state is signal loss ($\nexists\ \delta_t$), actually signal loss occupies a large portion among the measurements. The signal loss in the six measurements are shown in Table 6.8.

Basically, the signal loss failure can be detected by the GNSS receiver itself, the reference measurement system or the localisation unit. So the signal loss failures is accepted as safe failures.

6.5.6 Dangerous Failures to Faulty State

This kind of faulty is the faulty we need to deal with in most cases, the GNSS receiver location deviation is bigger than threshold δ_2, then it is a unacceptable deviation for train localisation on the medium density line.

In this situation, with the reference location, the GNSS receiver location deviation can be calculated. Similar to safe failures, the percentage of the dangerous failure to dangerous faulty state is calculated as shown in Table 6.9. Comparing the both table of the portion of safe faulty state and the dangerous faulty state, it is easy to see the safe failures play great role in all the faulty states.

Figure 6.18: Open Area Snapshot from *Nova Polianka* to *Danielov dom*

Since GNSS for train localisation is a safety-related application, it is necessary to investigate the dangerous failures in each environmental scenarios and identify the dangerous failure rates rather than the percentage of the dangerous faulty states in the whole faulty states quantitatively in accordance with the requirement in Table 5.5.

6.5.7 Dangerous Failure Rate in Open Area Scenario

Open area means there are almost no high dense trees or bridges along the railway track. As in the test track, between station *Danielov dom* and station *Novà Polianka* 0.87 km track can be treated as a short clip from open area. Figure 6.18 is shown as an example of open area scenario.

On 16 May 2008, the GNSS receiver locations were collected between the two stations for 4 times, the average time to travel between the two stations is 60 sec, one of the test run is shown in Figure 6.19. The mean value of HDOP is 1.4, the number of visible satellites is 6, the mean deviation for the 4 test runs is 5.43 m. There are no dangerous failures in open area during this day. The availability is estimated as 100%.

The whole test in May showed that in open area there are also some situations there is no GNSS signal (18 May 2008) or HDOP is too high (20 May 2008). The availability of this scenario is 95.78%. The dangerous failure rate of this scenario is:

$$\lambda_{D\_open\ area} = 5.22 \times 10^{-7}/h$$

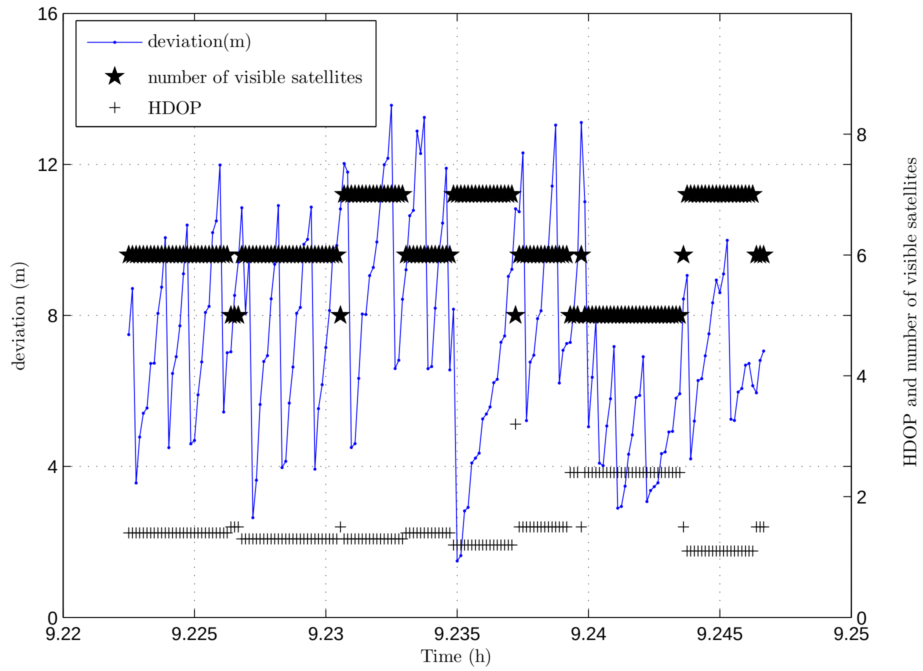


FIGURE 6.19: Number of Visible Satellites, HDOP, and Deviation in Open Area (16 May 2008)

Even not considering the diagnostic coverage, this dangerous failure rate still meets safety integrity level (SIL) 2. This dangerous failure rate needs to be compared with the requirement of the medium density line train localisation, then the acceptance of the GNSS receiver for train localisation can be made.

6.5.8 Dangerous Failure Rate in Forest Scenario

In High Tatra Mountains, there are a few clips of the tracks surrounded or even covered by trees, as shown in Figure 6.20. It is also a level crossing, the track is covered by trees.

The length of the track to be analysed is 1.12 km. There are 6 test runs through this scenario on 16 May 2008, and the average time for travelling through this forest is 99 s. The deviation and other parameters for one of the test runs are shown in Figure 6.21. As seen from the figure, the deviation goes up to 15.2 m, and the HDOP also goes greater than 6. Besides, there are also some timestamps no GNSS information at all. The availability is 10.33% for the all the test runs used earlier in this chapter.

FIGURE 6.20: Forest Snapshot between *Pod Lesom* and *Nova Lesna*

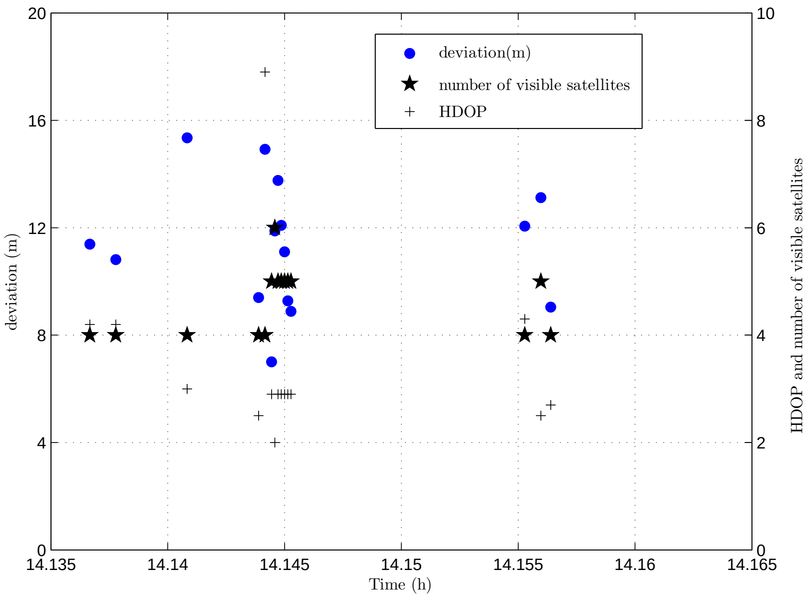


FIGURE 6.21: Number of Visible Satellites, HDOP, and Deviation in Forest (16 May 2008)

According to the requirement proposed in Table 5.5, for a medium density line, the alarm limit is 20 m. In the test run shown in Figure 6.21, there are no dangerous failures since all the deviation are smaller than 20 m. But considering other test runs, for example on 18 May 2008 also in forest scenario there are 10 measurement deviations greater than 20 m, which means 5 seconds. So the dangerous failure rate for the test runs evaluated is:

$$\lambda_{D\text{-}forest} = 5.25 \times 10^{-2}/h$$

The dangerous failure rate is really high at this scenario. Other localisation sensors should be installed as supplement to solve this critical situation. So a GNSS-based localisation unit is needed for forest scenario to perform safe train localisation.

6.6 Identification of Evaluation Results and Proposed Requirements

In Chapter 5, the properties of GNSS for train localisation are migrated. Then a quantitative requirement based on the existing values from the GNSS applications is proposed. The quantitative requirement is always mentioned in the numerical results of the performance evaluation. With the throughout evaluation of the characteristics in GNSS for train localisation, it is necessary to compare the evaluated results with the proposed requirement values.

The comparison of the proposed requirements and evaluation results is shown in Table 6.10. The accuracy is not comparable, because the evaluation result is using the proposed requirement of 10 m as the threshold for the up state. Without the threshold, the mean value will be much greater. Both the reliability and availability values of GNSS for train localisation in the test track do not meet the proposed requirements. In that the evaluated GNSS receiver location reliability is denoted in $MTTF$, not in failure rate, it is then converted to failure rate. As seen from the evaluation result, there is impossible for GNSS SPS receiver alone to provide always below 10 meters accuracy in the test track since the train is going through different environmental scenarios. Other localisation sensors are highly required together with GNSS SPS receiver to deliver more accurate locations in order to meet the proposed requirements.

Considering individual environmental scenarios, the evaluated safety integrity results are only in dangerous failures λ_D not as required λ_{DU}. Since for one system the $\lambda_D \geqslant \lambda_{DU}$, the dangerous failure rate in open area scenario meets the proposed requirement. The availability in open area is also greater than the generalised number show in the table, but still smaller than the proposed requirement. For forest, it is the other way round. The dangerous failure rate is already far greater than the required dangerous undetected failure rate.

The evaluated results show a very clear signal: using a stand-alone GNSS SPS receiver is not sufficient for train localisation application in each environmental scenario. But this evaluation methodology and process is still applicable for other localisation sensors for train localisation.

Table 6.10: Identification of Proposed Requirements and Evaluation Results

Properties	Characteristics	Proposed Requirements	Evaluation Results
Accuracy	95% confidence level	10 m	13.83 m
Reliability	failure rate	$\lambda_{all} < 2 \times 10^{-4}/\ h$	$\lambda_{all} \approx 19.46/\ h$
Availability	percentage	99.98%	82.26%
Safety Integrity	hazard rate	$\lambda_{DU} \leqslant 4.77 \times 10^{-6}/\ h$	varies in different environmental scenarios $\lambda_{D\_open\ area} \approx 5.22 \times 10^{-7}/\ h$ $\lambda_{D\_forest} \approx 5.25 \times 10^{-2}/\ h$

6.7 Chapter Summary

This chapter evaluates the four properties proposed in Chapter 5. Since the accuracy is the foundation of the other GNSS for train localisation properties, the reference measurement system is used to calculate the deviation between the GNSS receiver location and reference location. That is δ_t. δ_t inspires a total formalisation of the properties and proposed characteristics from Chapter 5.

The GNSS receiver locations are modelled into a stochastic Petri net model, the states of the model are: up state, degraded state, and faulty state. The states in the model help to identify the performance of GNSS receiver location. The states in the model also help the formalisation of the characteristics. The individual TTF_i is calculated, then the reliability and availability are evaluated based on it. The individual TTF_i is also plotted and fitted for the six transitions in the Petri net model. So the deviation δ_t identifies the three states, then derived TTF_i helps to estimate the firing rate distributions of the transitions in the Petri net model.

The successful formalisation of the characteristics in GNSS for train localisation generates the sample-based evaluation process. Real data collected in the High Tatra Mountains are evaluated using the introduced evaluation process. The evaluation parameters are using the proposed requirements in Chapter 5. After that, an identification between the proposed requirements and the evaluated results is carried out. The result shows that with a GNSS SPS receiver alone cannot meet the proposed requirements in general. This requires other localisation sensors together forming a GNSS-based localisation unit to deliver more accurate locations.

Chapter 7

GNSS-based Train Localisation Unit Performance Verification

The performance verification is to check whether the GNSS receiver measured train location can be trusted. The verification process requires the support of other localisation sensors, thus a GNSS-based train localisation unit is designed.

7.1 From GNSS Receiver to GNSS-based Localisation Unit

The GNSS receiver locations are normally not directly on the railway track, it is necessary to snap the GNSS receiver location to the track using the digital track map. Thus, the track-snapped location is generated. The track-snapped location needs to be verified together with other localisation sensors to see whether it can be accepted as a safe train location. That is the necessity to move from a stand-alone GNSS SPS receiver to a GNSS-based localisation unit.

7.1.1 From External Evaluation to Internal Operation

The evaluation of the GNSS receiver performances has been issued in Chapter 6 through the help of the reference measurement system. The reference measurement system is an external source to understand the GNSS receiver performance. In railway systems, building the whole reference system along the track costs too much. The evaluated results represent the GNSS receiver location performance in general and also in different environmental scenarios. The evaluated results of the GNSS for train localisation can be used for internal operation.

Table 7.1: Four Types of Locations, POI, and Distance

No.	Location Name	Abbreviation
1	GNSS receiver location	**G**
2	track-snapped location	**M**
3	localisation unit location	**L**
4	reference location	**R**
5	distance of track-snapped location and GNSS receiver location	**D**
6	POI in digital track map	**POI**

The internal operation uses other train localisation sensors together with the GNSS receiver and the studied GNSS receiver performance to execute the real-time verification of the measured GNSS receiver location. There is also a special advantage of railway than other means of transportation, the railway tracks. The railway tracks are already determined when the tracks are constructed, the track information can be also applied in the internal operation phase for GNSS receiver location verification.

7.1.2 Four Types of Locations

The GNSS receiver generates GNSS receiver location. Through the track-snapping process, the track-snapped location is generated. Then with the verification process, the localisation unit will deliver the localisation unit location. The external evaluation part, the reference measurement system generates the reference location together with the GNSS receiver location. These four locations are actually all train locations, but measured or estimated by different systems or algorithms.

To provide a clear written expression for mathematical equations, the GNSS receiver location, track-snapped location, localisation unit location, and the reference location are defined as the abbreviations in Table 7.1.

So, let $\mathbf{G}_i = (x_{i,G},\ y_{i,G})|_{i=1\ldots n}$ be vector of GNSS receiver location at time i, i is the timestamp.

Let $\mathbf{POI}_j = (x_{j,POI},\ y_{j,POI})$ be the vector of the POI in the digital track map, j is the POI ID.

Let $\mathbf{M}_i = (x_{i,M},\ y_{i,M})|_{i=1\ldots n}$ be vector of the track-snapped location at time i of GNSS receiver location $\mathbf{G}_i$ to the digital track map based on the **POI** polygon.

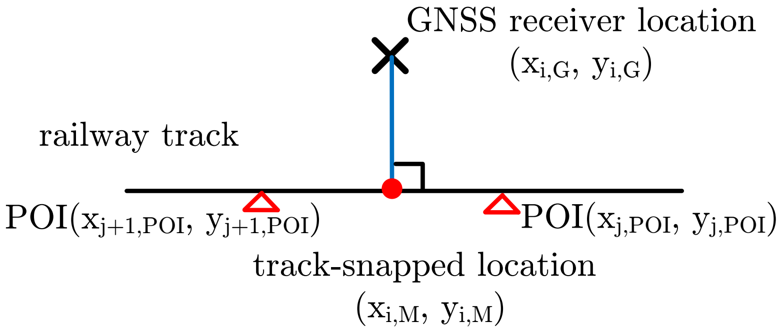


FIGURE 7.1: GNSS Receiver Location Track-snapped to the Railway Track

Thus, $\mathbf{D}_i = \overrightarrow{G_iM_i} = (x_{i,D},\ y_{i,D})|_{i=1...n}$ be vector of the distance between GNSS receiver location and the track-snapped location, in that i is the same timestamp as $\mathbf{G}_i$.

Let $\mathbf{R}_i = (x_{i,R},\ y_{i,R})|_{i=1...n}$ be vector of the reference locations of each GNSS receiver location $\mathbf{G_i}$.

In Chapter 6, the GNSS receiver performance evaluation is based on the deviation between reference $\mathbf{R_i}$ and GNSS receiver location $\mathbf{G_i}$. This chapter will consider more about the distance between the GNSS receiver location $\mathbf{G_i}$ and track-snapped location $\mathbf{M_i}$, that is $|\overrightarrow{G_iM_i}|$.

7.1.3 From GNSS Receiver Location to Track-snapped Location

The GNSS receiver location, track-snapped location, and the localisation unit location compose the whole localisation process of the train localisation by means of GNSS-based localisation. The first step is to get the track-snapped location from the GNSS receiver location, this requires the digital track map.

With the digital track map the measurement of the distance between GNSS receiver location and the track-snapped location $|\overrightarrow{G_iM_i}|$ is similar to the measurement of GNSS receiver location with reference location δ_i. The track-snapping process is illustrated in Figure 7.1. Without the reference measurement system, the **POI**s stored in the digital track map is the resource to snap the GNSS receiver location to the railway track correctly.

The components in the map are basically points, points compose lines, lines form the map. So a basic track snapping problem can be treated as a point to point, point

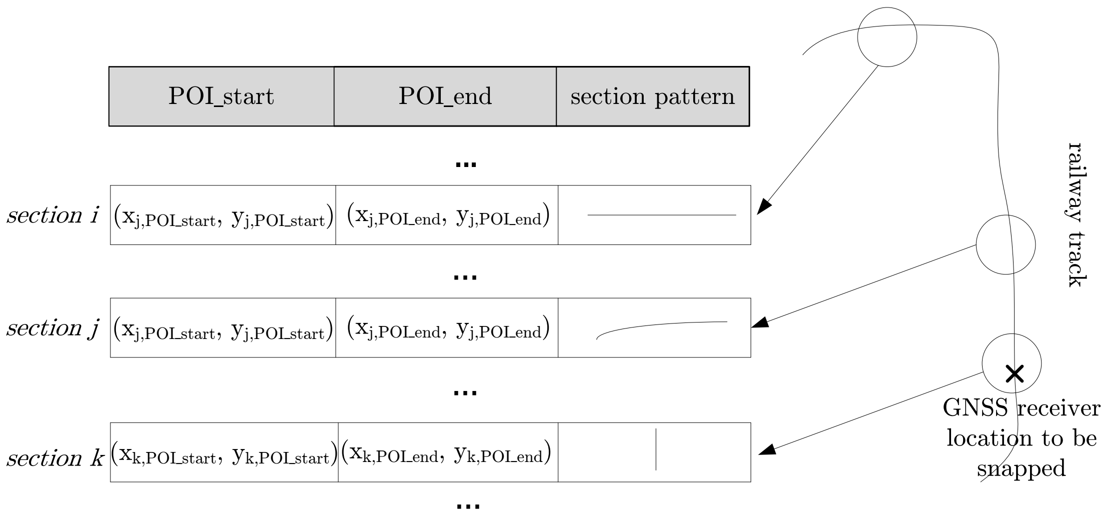


FIGURE 7.2: GNSS Receiver Location to Be Snapped into Track Section

to line, or line to line problem. Both point to point and point to line problem can be regarded as the search problem, and the line to line problem can be treated as a statistical estimation problem. With the available digital track map, it provides the constrains of the localisation space. A train is only possible to run on the railway track and unlikely to go other places. The cartographic information of the map described in Chapter 4 is considered as a set of sections formed by POIs. Each section comprises a start POI and an end POI, with several intermediate nodes.

The track map structure has already been defined clearly in Chapter 4 Figure 4.4. In the defined structure, the digital track map is divided into track sections, each track section is composed by nodes. A list of all the sections is used for a rough track snap. The GNSS receiver location is compared with the section POIs to find the appropriate section of the GNSS receiver location as shown in Figure 7.2. The binary search algorithm (also called half-interval search) is applied. At every step, the GNSS receiver location is compared with the section POIs, the minimum two distances are adopted for the next step. Finally only one section is left.

After the section has been determined, the nearest nodes for the GNSS receiver location are estimated according to a characteristic of the section. Each track section is divided with a single direction without circuity, which means when the GNSS receiver location is attributed to a track section, the track-snapped location is always between two POIs and also between two inner nodes in each track section.

Assume the GNSS receiver location to be located is G_i, the two track section POIs found with the binary search algorithm are $POI_{j_{start}}$ and $POI_{j_{end}}$. Inside the section, there are nodes called $node_k = (x_{k,node}, y_{k,node})$ in that $\{k = 1, ..., m\}$. The track-snapped location M_i is located in two adjacent nodes k and $k+1$ $(1 \leqslant k \leqslant m-1)$, when:

$$\frac{x_{i,G} - x_{k,node}}{x_{i,G} - x_{k+1,node}} < 0$$

or

$$\frac{y_{i,G} - y_{k,node}}{y_{i,G} - y_{k+1,node}} < 0$$

With this basic rule, a second binary search algorithm in the specified section is done until the adjacent nodes in the digital track map is found. The flow chart of the algorithm is shown in Figure 7.3. This shows both the track section matching and the node matching. With the track-snapping algorithm, the track-snapped location M_i can be correctly located into two adjacent nodes. Nodes and POIs are actually in the same format in the Gauss-Krüger coordinate. So for simplicity, both $node_k$ and POI_j are treated the same in this dissertation later as POI_j.

With the correct decision of the adjacent two nodes, denoted as POI_k and POI_{k+1}, the track-snapped location M_i can be determined according to two vector properties:

- If two vectors $\overrightarrow{a}$, $\overrightarrow{b}$ are orthogonal, then $\overrightarrow{a} \cdot \overrightarrow{b} = 0$.
- If two vectors $\overrightarrow{a}$, $\overrightarrow{b}$ are parallel, then $\overrightarrow{a} \times \overrightarrow{b} = \overrightarrow{0}$, thus the determinant of the two vectors $det(\overrightarrow{a}, \overrightarrow{b}) = 0$

So with the vector properties, it has the following equation:

$$\begin{cases} \overrightarrow{G_iM_i} \cdot \overrightarrow{POI_jPOI_{j+1}} = 0 \\ det[\overrightarrow{POI_jM_i}, \overrightarrow{POI_jPOI_{j+1}}] = 0 \end{cases} \tag{7.1}$$

Expand the equation array in Equation 7.1, the GNSS receiver location track-snapped to the track can be calculated as in the form of $\mathbf{A}x = b$ to calculate

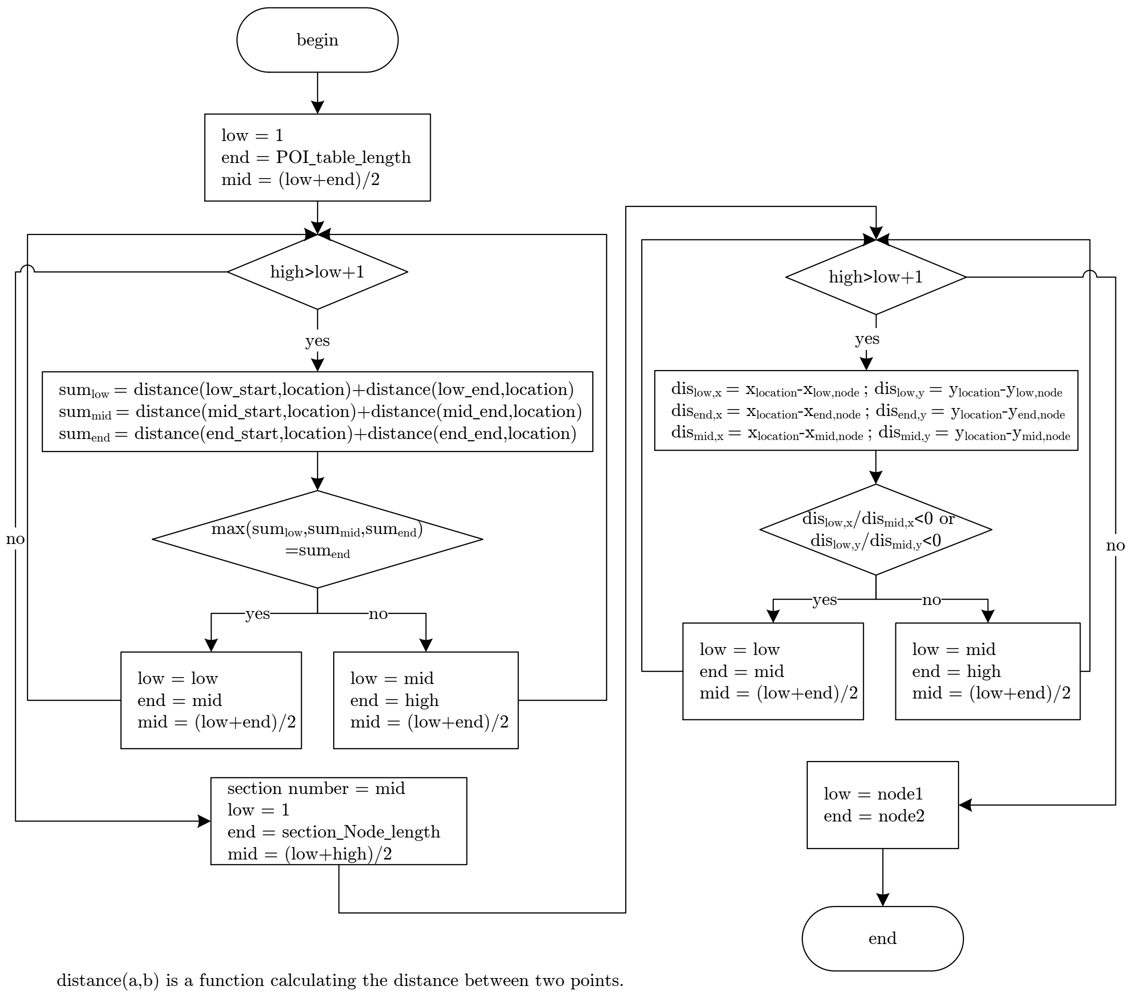


FIGURE 7.3: GNSS Receiver Location Nodes Decision Flow Chart

the $\mathbf{M}(x_{i,M},\ y_{i,M})$:

$$\begin{bmatrix} x_{j+1,POI} - x_{j,POI} & y_{j+1,POI} - y_{j,POI} \\ y_{j+1,POI} - y_{j,POI} & -(x_{j+1,POI} - x_{j,POI}) \end{bmatrix} \begin{bmatrix} x_{i,M} \\ y_{i,M} \end{bmatrix}$$

$$= \begin{bmatrix} x_{i,G} & y_{i,G} \\ -y_{j,POI} & y_{j,POI} \end{bmatrix} \begin{bmatrix} x_{j+1,POI} - x_{j,POI} \\ y_{j+1,POI} - y_{j,POI} \end{bmatrix}$$

$$= \begin{bmatrix} x_{i,G} \cdot (x_{j+1,POI} - x_{j,POI}) + y_{i,G} \cdot (y_{j+1,POI} - y_{j,POI}) \\ -y_{j,POI} \cdot (x_{j+1,POI} - x_{j,POI}) + y_{j,POI} \cdot (y_{j+1,POI} - y_{j,POI}) \end{bmatrix}$$

In the equation, define:

$$x_{j+1,POI} - x_{j,POI} = \Delta x_{POI}$$

and

$$y_{j+1,POI} - y_{j,POI} = \Delta y_{POI}$$

the equation is simplified as:

$$\begin{bmatrix} \Delta x_{POI} & \Delta y_{POI} \\ \Delta y_{POI} & -\Delta x_{POI} \end{bmatrix} \begin{bmatrix} x_{i,M} \\ y_{i,M} \end{bmatrix} = \begin{bmatrix} x_{i,G} \cdot \Delta x_{POI} + y_{i,G} \cdot \Delta x_{POI} \\ -y_{j,POI} \cdot \Delta x_{POI} + y_{j,POI} \cdot \Delta x_{POI} \end{bmatrix} \tag{7.2}$$

With the calculated $\mathbf{M}_i$, each GNSS receiver location $\mathbf{G}_i$ is attributed to a track-snapped location on the track.

7.2 Architecture of the GNSS-based Localisation Unit

The verification process calls for several localisation sensors together to compose the GNSS-based localisation unit.

7.2.1 Redundancy and Voting Structure

Redundancy is the inclusion of extra critical components of a system with the intention of increasing reliability of the system, usually in the instance of a backup or fail-safe. Redundancy is also named as voting logic. In GNSS for train localisation, the information redundancy is used for GNSS receiver location dangerous faulty state detection. This information redundancy provides elimination performance declension by monitoring performance of individual components, and this monitoring is used in voting logic.

The voting logic includes at least two components, they are primary and alternative component. They both give similar output, but the output of the alternative component remains inactive during normal state (up and degraded states). The action of the alternative component depends on the voting scheme. When the primary detects a fault, the alternative component can either take over the function from the primary component, or cause the output of the system to be off.

As advised from IEC 61508-6, in the continuous mode of operation, a 1oo2, 1oo2D, 2oo2, and 2oo3 are needed. For 1oo2, 1oo2D, 2oo2, and 2oo3 components or subsystems, it is assumed that any repair is on-line [17]. If an E/E/PE safety-related system is configured such that on any detected fault the EUC is put into a safe state, then the probability of failure on demand will be improved. The degree of improvement will be dependent on the diagnostic coverage. An example of the two

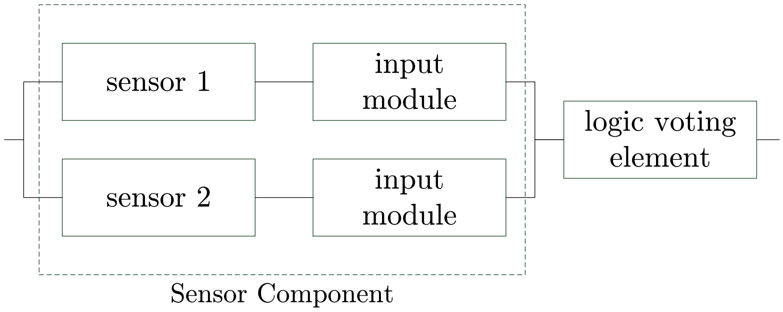


Figure 7.4: Example of Two Sensors Configuration

channel sensor component configuration is listed in Figure 7.4. This structure has been structurally verified as safe for train localisation, also based on a Petri net model in a previous paper written by the author of this dissertation [150].

7.2.2 GNSS-based Localisation Unit Design

The verification of a safe train location can be done through voting of the measured train location from two independent sources. The Doppler radar and the GNSS receiver both deliver velocity measurements but not affected by each other.[16]

The GNSS receiver not only provides location measurement of the moving object, but also provides velocity measurement using Doppler effect of the moving object, this could have common cause failure from the GNSS transmitted signals. But from the measurement principles, the error source affecting GNSS receiver locations are not related to GNSS receiver velocities [151]. The common cause failure is in the situation that there are no GNSS signal, as stated in the evaluation methodology it is regarded as a safe failure.

To implement the voting structure, another sensor to measure the train velocity is needed. The Doppler radar can be used. The principle of the Doppler radar velocity measurement and GNSS receiver velocity measurement are similar. But they are not affected by each other.

With one GNSS receiver and one Doppler radar, the voting structure of the train velocity is settled. Then the acknowledged train velocity at time $t(i)$ together with acknowledged train location at time $t(i-1)$ can estimate the next train mileage according to the direction of the train. This estimated train mileage can be used

[16]Doppler radar velocity measurement is in the object body coordinate, GNSS receiver velocity measurement is in the navigation coordinate. The coordinates are different, in this dissertation the velocity measurements from the two coordinates shows high conformability, so the velocity measurements are used without conversion.

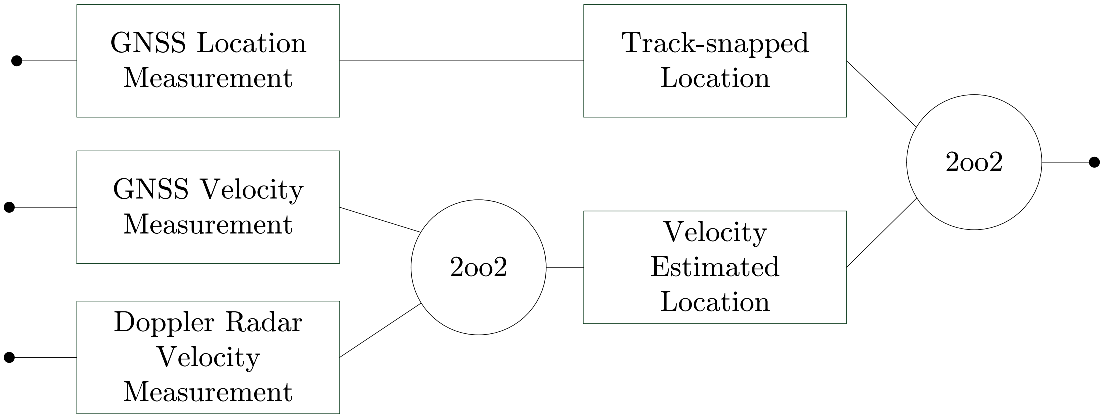


Figure 7.5: Two Layer 2oo2 GNSS-based Localisation Unit Structure in Reliability Block Diagram

together with the independent map-matched location from the GNSS receiver and the digital track map to form another voting structure of the train location. This is a two layer 2oo2 structure, as shown in Figure 7.5.

This two layer 2oo2 structure uses three resources and then compares the resources to determine the correct train location. They are the pseudorange measurement, the Doppler effect by the GNSS signal transmission, the Doppler effect by the microwave transmitted from the Doppler radar. The diversity of the voting scheme reduces the probability of systematic or common cause dangerous failures affecting the reliability and availability of the system.

7.3 Verification Methodologies for the Locations

The two layer 2oo2 has two voting logic schemes. The hardware redundancy voting logic compares the two sources of input, when the two inputs are exactly the same, then the 2oo2 structure can deliver a safe result. But there will be small differences in value between the GNSS receiver measured train velocity and Doppler radar measured train velocity, so a hypothesis testing based voting logic is introduced.

There are three hypothesis testings for location verification: testing of GNSS receiver location on the track, testing of GNSS receiver velocity same as Doppler radar velocity, testing of track-snapped location same as the estimated location. After these three steps, the localisation unit train location can be trusted and accepted. The whole procedure can be explained in the Petri net model clearly through Figure 7.6.

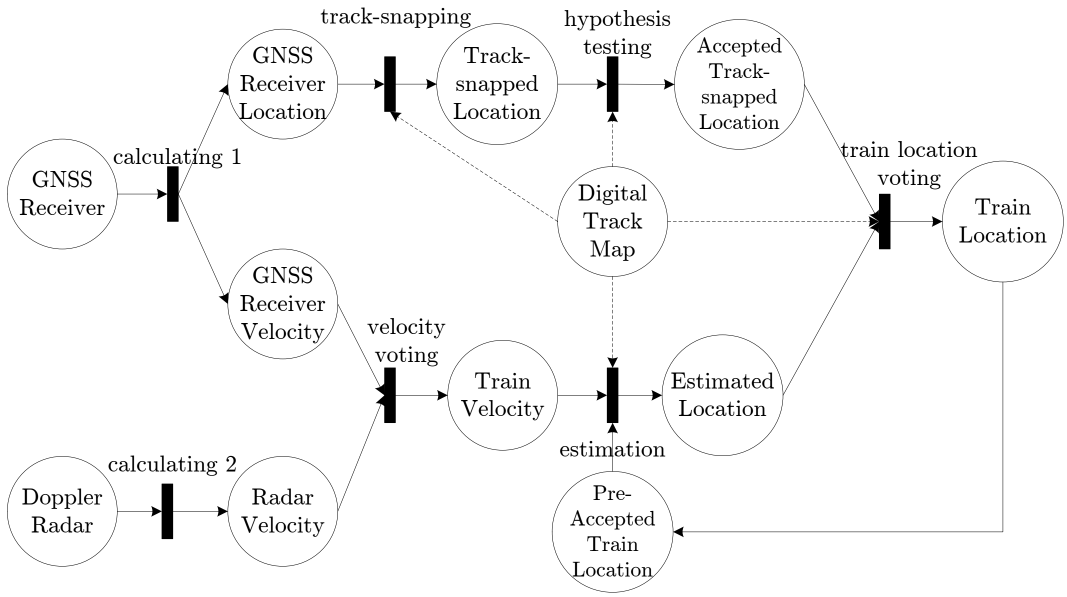


FIGURE 7.6: Two Layer 2oo2 GNSS Location Verification Structure in Petri net

7.3.1 Verification of GNSS Receiver Location on the Track

Considering the process of GNSS receiver location G_i to track-snapped location M_i, the distance $|D_i| = |\overrightarrow{G_iM_i}|$ should be as reasonably low as possible. This distance can be treated as perpendicular deviation of the GNSS receiver location. When the perpendicular deviation is acceptable, then the GNSS receiver location can be accepted as on the track.

This hypothesis testing is to test whether the perpendicular deviation is acceptable. The best result is that $|D_i| = |\overrightarrow{G_iM_i}| = 0$, but it is normally not in the case. A specific threshold can be adopted as acceptable, namely $D_0 = \mu \pm 2\sigma$ as the 95% of the normal distribution. So the hypothesis testing of GNSS receiver location on the track can be set as:

- null hypothesis: $H_0 : |D_t| \leqslant \mu \pm 2\sigma(D_0)$,
- alternative hypothesis: $H_1 : |D_t| > \mu \pm 2\sigma(D_0)$.

In hypothesis testing it is called *directional test* or *one-tailed test*.

One directional GNSS receiver locations can be regarded as normal distribution.[17] So actually, the perpendicular deviation to the track of the GNSS receiver locations can be assumed as a point belong to the normal distribution function. The origin

[17]For different measurements, different distributions can be fitted. Normal distribution is used as the most common distribution among these distributions.

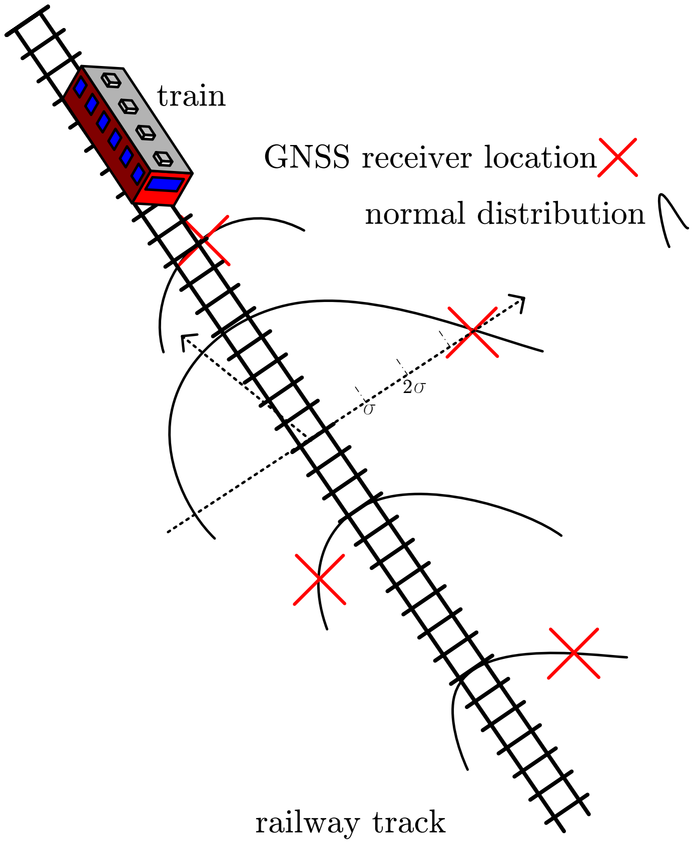


FIGURE 7.7: GNSS Receiver Location on the Track Hypothesis Testing

of the distribution coordinate should be located on the snapped railway track. This relation can be shown in Figure 7.7.

For GNSS receiver location real-time hypothesis testing, only a small amount of GNSS receiver locations sample can be used. For testing of a small sample, one way is to test the mean value, the other way is to test the variance. Using variance is based on the assumption that the mean value is not suitable to be used for hypothesis testing.

In the evaluation results, the mean value μ_0 and the variance σ for the up state is already determined with a large number of measurement samples. This can be used as a parameter for the hypothesis testing. But since GNSS receiver location accuracy varies in different environments, the traditional $z-test$ is not suitable to be used as a test statistic for this application. Based on the real-time small samples, the standard deviation of the small samples can be used as the parameter for the test statistic. So the test statistic can be created as:

$$t = \frac{|D_t| - D_0}{s/\sqrt{n}}$$

In that, D_0 is using the evaluation results of the accuracy evaluation of the 95% from Chapter 6. s is using the small sample with $n = 5$.

So when H_0 is true, $t \sim t(n-1)$ is a t-distribution. The rejection region for directional testing is:

$$P_{H_0}\{|t| \geqslant t_\alpha\} = \alpha$$

The rejection region is regarded as:

$$C = \{|t| \geqslant t_\alpha\}$$

In that $\alpha = 0.05$ in consistency with the significance level.

7.3.2 Voting of GNSS Receiver and Doppler Radar Velocities

Considering the GNSS receiver velocity $\mathbf{V_t}$ and Doppler radar velocity $\mathbf{R_t}$ measured at the same time t. they are two samples with $n_V = n_R = n$ when there are no signal loss.

Remark 7.1 **R** Interpretation
In this section **R** is used as the velocity measurement from the Doppler radar, considering the performance evaluation in Chapter 6 the **R** is used as the abbreviation for reference location. This section is using **R** intentionally. The two samples hypothesis testing can be applied to test the measurement consistency of GNSS receiver velocity **V** and radar velocity **R**. It will also be used to test the measurement consistency of GNSS receiver location **G** and reference location **R**. By this means, they are interchangeable.

Considering the GNSS receiver velocity **V** and the radar velocity **R**, it is applied as every timestamp of **V** there is always a radar velocity **R**. So they are generated at the same time, and it is suitable to apply two samples hypothesis test.

For GNSS receiver velocity and radar velocity, the hypotheses are:

- null hypothesis $H_0 : E(v_i - r_i) = 0$ is interpreted as the GNSS receiver velocity is the same as the radar velocity,

- alternative hypothesis $H_1 : E(v_i - r_i) \neq 0$, which means the measurement of GNSS receiver and radar velocities are different, and it cannot be used for train localisation purpose.

This test is for every $i = 1 : n$ for each GNSS receiver velocity and the corresponding radar velocity measurement. The two measurement samples v_i and r_i can be considered as both the mean value and variance unknown beforehand. So the two samples unknown mean value and unknown variance can be adopted for the t test statistic. According to a study of the collected GNSS receiver velocity and Doppler radar velocity, the variance of both velocities can be treated as the same in the measurement sample. So $\mathbf{V}$ and $\mathbf{R}$ are considered as having $\sigma_V^2 = \sigma_R^2 = \sigma^2$, the test statistic can be taken as:

$$T = \frac{\overline{x_v} - \overline{x_r}}{s_\omega \sqrt{\frac{1}{n_v} + \frac{1}{n_r}}} = \frac{\overline{x_v} - \overline{x_r}}{s_\omega \sqrt{\frac{2}{n_v}}} \tag{7.3}$$

in that,

$$s_\omega^2 = \frac{(n_v - 1)s_v^2 + (n_r - 1)s_r^2}{n_v + n_r - 2} = \frac{s_v^2 + s_r^2}{2} \tag{7.4}$$

Considering Equation Equation 7.3, when H_0 is true:

$$T = \frac{\overline{x_v} - \overline{x_r}}{s_\omega \sqrt{\frac{2}{n_v}}} \sim t(2n_v - 2) \tag{7.5}$$

That is to say the test statistic follows student t-distribution when H_0 is true. With the accepted velocity, the result of the first layer 2oo2 can be transferred to the second layer 2oo2.

7.3.3 Voting of Estimated and Track-snapped Locations

At time $t-1$, the accepted localisation unit location L_{t-1} and the voted velocity as V_{t-1} are both used to estimate the localisation unit location $L_t^{'}$ at time t. The estimation process of $L_t^{'}$ is as follows:

1. Determine the travelling direction of the train;
2. Determine the mileage at time t according to L_{t-1};
3. Determine the estimated mileage of $L_t^{'}$ according to L_{t-1} and V_{t-1}.

At time t, the measured GNSS receiver location G_t is track-snapped to the railway track as track-snapped location M_t. So at time t, the estimated train location $L_t^{'}$ and the track-snapped location M_t needs to be verified to see whether both are the same with each other. This is the second layer 2oo2 voting.

Similar to the velocity voting, the "two sample unknown μ and unknown σ" hypothesis testing can be applied. The hypotheses are:

- null hypothesis: $H_0 : |\overrightarrow{L_t^{'}L_t}| = 0$,
- alternative hypothesis: $H_1 : |\overrightarrow{L_t^{'}L_t}| \neq 0$.

This voting scheme concludes the acceptance of the train location measurement by the GNSS-based localisation unit.

7.4 Safety Margin Estimation

After the successful verification of the GNSS receiver location, then the successful voting result implemented by the localisation unit, the acceptable localisation unit location is generated as safe train location. Based on the safe train location, the safety margin for this train location can be estimated for moving block train control system. The definition of safety margin is as follows:

Definition 7.1 Safety Margin [9]
A safety margin is a zone for the current train that no other trains are allowed to enter.

To determine the safety margin, the driving direction of the train, the velocity of the train, the length of the train, and the braking distance of the train are all needed as pre-information. And as already seen from the evaluation results, the environmental scenarios play great role on affection of GNSS receiver location accuracy level. Since the safety margin estimation is related to location measurement accuracy level, it is also related to environmental scenarios [33].

The evaluation of GNSS receiver location accuracy is based on $\delta_t = |\overrightarrow{G_tR_t}|$. Then the perpendicular accuracy is considered for GNSS receiver location on the track verification, that is $|D_t| = |\overrightarrow{G_tM_t}|$. Now for safety margin generation, along the track accuracy (or 1D accuracy) is required, that is $\Delta_t = |\overrightarrow{L_tR_t}|$. The trusted train location L_t and the trusted reference location R_t are both on the track, thus Δ_t shows the deviation of on the track. Large number of samples can be evaluated to get the parameter for each environmental scenario. The standard deviation for each environmental scenario can be finally attributed as in Table 7.2.

TABLE 7.2: Standard Deviation Estimation of S_t in Different Environmental Scenarios

No.	Environment	Standard Deviation
1	Open Area	σ_{1,Δ_t}
2	Forest	σ_{2,Δ_t}
3	Tunnel	no information
4	...	...

In consideration of appropriate parameters, the safety margin[18] can be estimated according to:

$$Safety\ Margin(t) = K_t \times HDOP_t \times \sigma_{i,\Delta_t} + S_{braking\ curve} \tag{7.6}$$

In that, i is the environmental scenario number from Table 7.2, the first part of the equation forms the GNSS specific safety margin. K_t is determined according to a mean value in the last 10 measurements in real time, $HDOP_t$ is the value of the current measurement[19], $S_{braking\ curve}$ is the braking curve of the current train.

With the estimated safety margin in Equation 7.6, the trains are achieving the safety goals by being constrained on the track.

One thing still needs to mention, this section only introduces the possible methodologies to generate the safety margin for GNSS-based train localisation, the numerical results of safety margin for each voted train location is not estimated because of lacking the information of the train model, train braking curve information, etc.

7.5 Numerical Results of Performance Verification

The data for performance verification is also the data collected in the High Tatra Mountain railway line. Since the reference location is not used for performance verification, the data collected by Doppler radar is used as the information for the other sensor in the GNSS-based localisation unit.

[18] This safety margin estimation is the first approach as a suggestion for calculating the margin. The actual calculation is not presented in this dissertation, and the parameters may need to be modified or improved for further calculations.

[19] Since the HDOP is used for safety margin calculation, the safe aspect of HDOP also needs to be calculated.

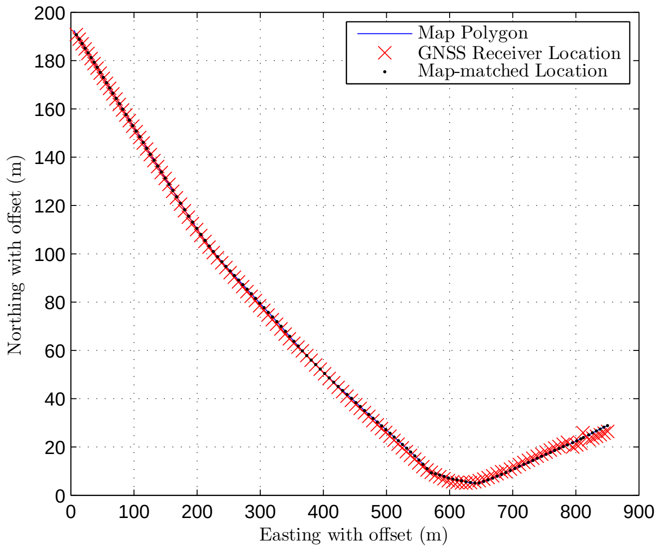


FIGURE 7.8: A Short Clip of GNSS Receiver Location, Track-snapped Location, and Map Polygon in Open Area Scenario

7.5.1 GNSS Receiver Location Track-snapping

The measurement on 16 May 2008 is used for the track-snapping procedure. The complete GNSS receiver location in a test run is too large to see the track-snapped result in detail, so a data clip in open area scenario with 141 samples is used as an example in Figure 7.8. In this clip the train was approaching a railway station, then stopped in the station for several seconds, and then moved to another station. In that, only one GNSS receiver location has big perpendicular distance, the other GNSS receiver locations are all acceptable on the track.

Another data clip in forest scenario is shown in Figure 7.9. Signal loss is still the biggest problem in forest scenario. The GNSS receiver locations compared with the ones in open area scenario are a little bit far away from the corresponding track-snapped locations on the track.

Both the open area scenario and the forest scenario are drawn with offsets in the Gauss-Krüger Easting and Northing for easier reading of the distances. The following location measurement figures are all displayed with offsets.

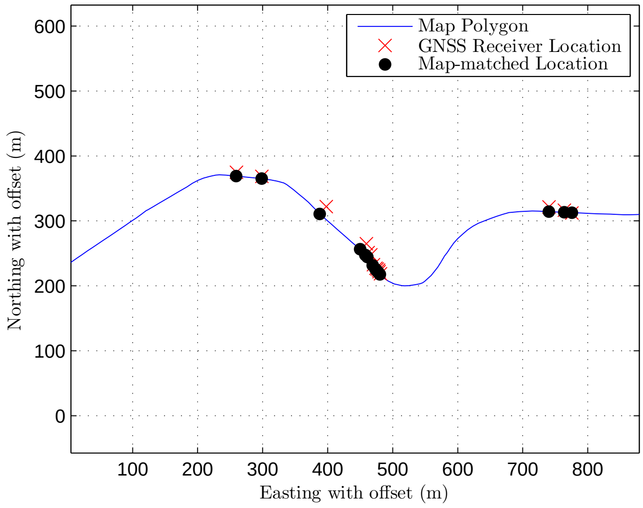


FIGURE 7.9: A Short Clip of GNSS Receiver Location, Track-snapped Location, and Map Polygon in Forest Scenario

7.5.2 Hypothesis Testing of GNSS Receiver Location on the Track

The test statistic to test the GNSS receiver location on the track is built as:

$$t = \frac{x - D_0}{s/\sqrt{n}}$$

In that, $D_0 = 13.83\ m$ as adopted from the evaluated accuracy information for up state. For each GNSS receiver location, the test is based on

$$H_0 : |D_t| \leqslant 13.83 \ \leftrightarrow \ H1 : |D_t| > 13.83$$

The rejection threshold for not accepting GNSS receiver location on the track should be:

$$C \ = \ \left\{ \frac{|D_t| - 4.54}{s/\sqrt{n}} > t_\alpha(n-1) \right\}$$

in that $\alpha = 0.005$.

The hypothesis testing results are both concerning two environmental scenarios. The open area scenario, as shown in Figure 7.8, the GNSS receiver locations are all accepted as on the track, so the figure for the hypothesis testing result in open area is not shown in this part. But the hypothesis testing result in forest scenario is shown in Figure 7.10. In that figure, the five-pointed stars are the GNSS receiver locations not acceptable as on the track. This result proves further that the environmental scenarios need to be considered for the GNSS-based localisation applications.

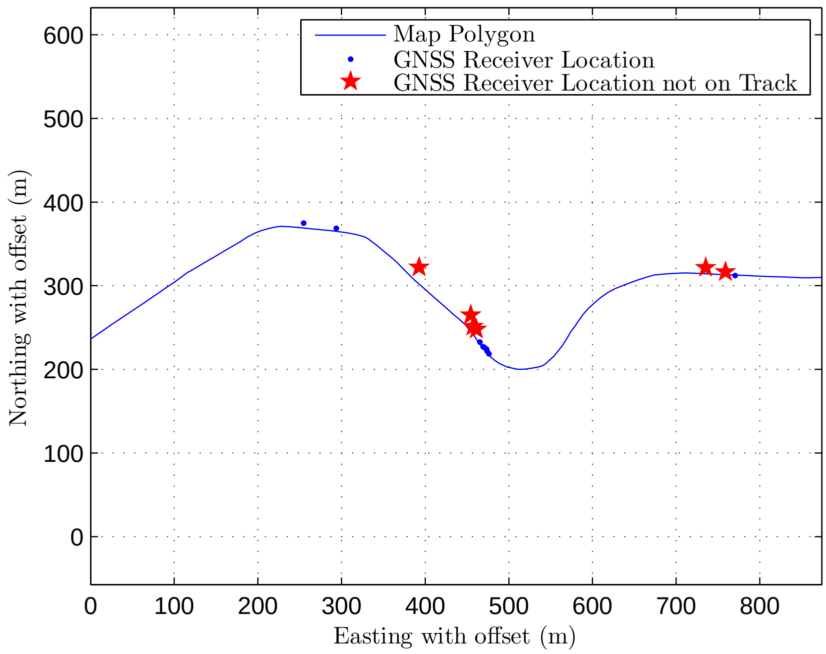


FIGURE 7.10: GNSS Receiver Location on the Track Hypothesis Testing in Forest Scenario

It is also necessary to test the performance of the hypothesis testing algorithm, that is to test the detection ratio (λ_{DU}) and false alarm (λ_{FA}) of the algorithm. As stated by optimal detection theory, the detection for a safety-related system will have detected and undetected failures. For this purpose, a large samples clip is used for testing the hypothesis testing algorithm performance. The verification methodology gives the acceptance of the GNSS receiver location. Meanwhile, the reference measurement system and GNSS receiver delivers the δ_t, it compares with the specification for the medium density line, the acceptance of GNSS receiver location can also be made. The two detections can be compared.

Figure 7.11 shows the big deviation $\delta_t > d_2$ by the reference on the upper figure, then shows the hypothesis testing results of the GNSS receiver location not acceptable on the track on the under figure. The testing results in Figure 7.11 show that each GNSS dangerous faulty states are detected by the testing algorithm.

More samples are analysed for a statistical representation of the hypothesis testing algorithm in Table 7.3. The hypothesis testing algorithm of GNSS receiver location on track verification results show that the safe failures are all detected, no up or degraded states are false detected as signal loss. The λ_{DU} is evaluated as 1.37×10^{-4} / hour, and for the false alarm, the algorithm could have 14 false alarms per

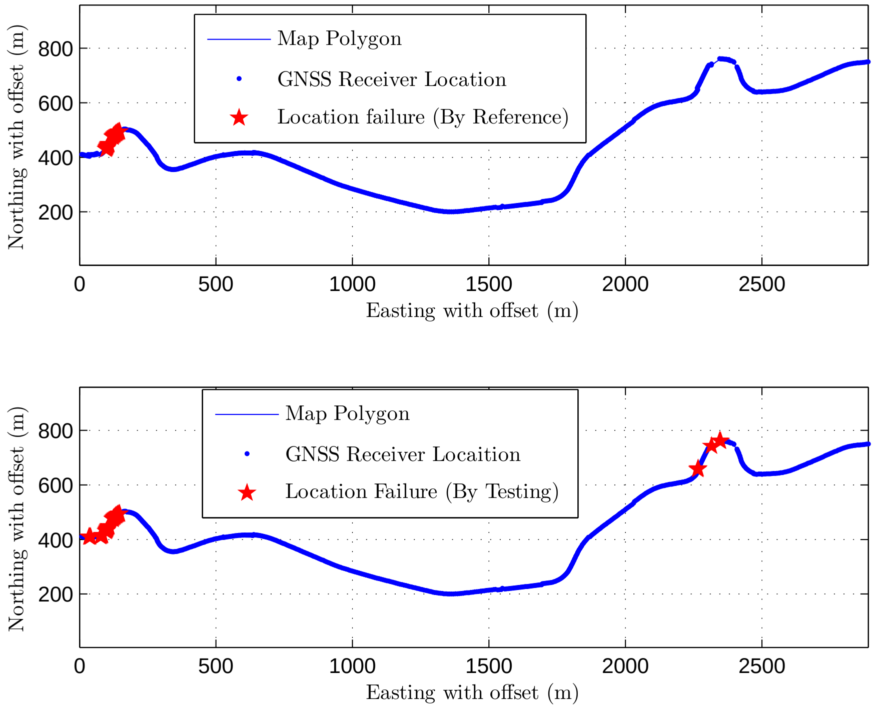


FIGURE 7.11: GNSS Receiver Location Hypothesis Testing of on the Track Overview

TABLE 7.3: Statistical Results for the Hypothesis Testing Algorithm

	Category of Failure Rate	Rate
$\nexists\ \delta_t$	safe undetected failure rate λ_{SU}	0
	up or degraded as safe failure rate λ_{FA}	0
$\delta_t > D_0$	dangerous undetected failure rate λ_{DU}	1.37×10^{-4} /hour
	up or degraded as dangerous failure rate λ_{FA}	1.40×10^{1} /hour

hour, which is a little bit too high, but not causing safety problems, since they are detected. But this will cause lower reliability performance of the localisation unit.

7.5.3 Two Layer 2oo2 Voting of Velocities and Locations

There are two voting schemes, the first is velocity voting, the second is location voting. They are shown in Figure 7.12. The data in the figure is in a open area scenario.

Velocity voting is the basic comparison of V_t and R_t, the test result in this sample clip shows that there are two measurements different from each other. So these two

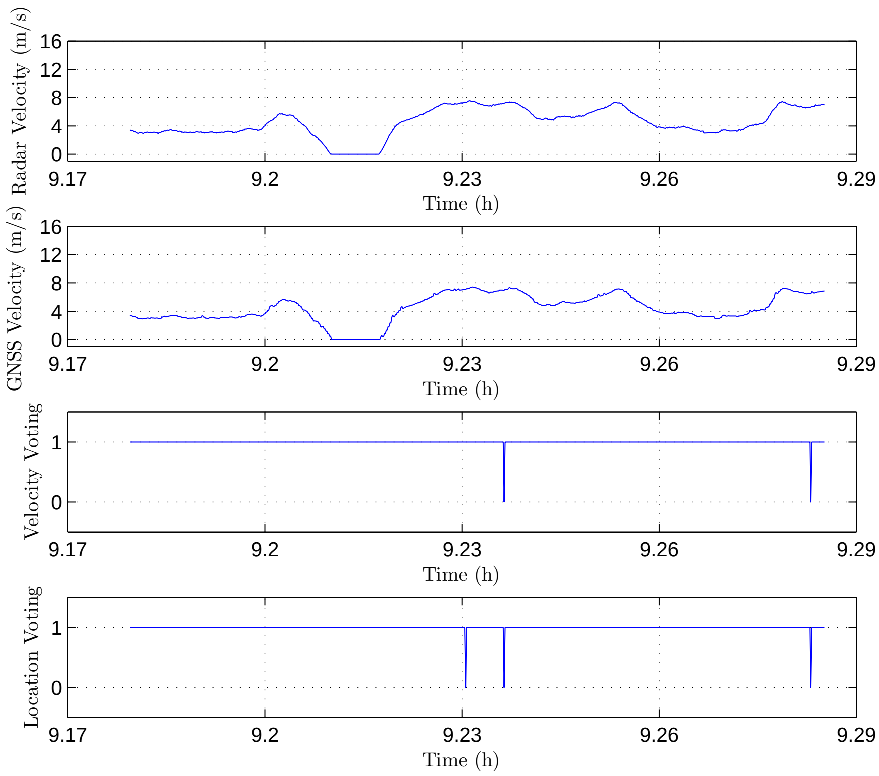


FIGURE 7.12: GNSS Receiver Velocity, Doppler Radar Velocity, Map-matched Location Two Layer 2oo2 Voting

velocity measurements can not be trusted. Then for location voting, the maximum $|\overrightarrow{L_t^{'}L_t}|$ value is 5.34 m. This process brings one sample as not acceptable. This result shows that the two layer 2oo2 can be used for real-time verification of the safe train location.

7.6 Chapter Summary

The objective of the performance verification methodology is to show how to trust the measured train location in real time. Thus the GNSS receiver is integrated into a GNSS-based localisation unit to provide self verification of the measurements by different sensors.

The self verification requires the digital track map instead of the external reference measurement system. The method to match the GNSS receiver location on the track is introduced. Then the necessity of the GNSS-based localisation unit is designed for the purpose of delivering safe train locations based on voting scheme.

In the structure of the localisation unit, there are three steps of verification. The first verification is to verify the GNSS receiver locations to be acceptable on the track. This is to verify $|D_t| = |\overrightarrow{G_t M_t}|$ to be as low as required using the evaluation results from the last chapter. Then the following two steps are identical with the two layer 2oo2 voting scheme. The two layer 2oo2 voting scheme is basically to check whether the two outputs are the same using the hypothesis testing methods. This is using a two samples unknown mean value unknown variance hypothesis testing method. The performance of the verification processes are tested using the data collected in the High Tatra Mountain railway line.

These three parts forms the real-time verification process of the GNSS for train localisation. This answers the question proposed in the purpose of the dissertation of how to apply GNSS GNSS into train localisation according to the related standards, specifications, and advisories, and then generate a safe train location for the purpose of train control.

Chapter 8

Conclusions and Recommendations

The following Section 8.1 states conclusions for whole process from terminology migration, to performance evaluation, till performance verification introduced in this dissertation. After that, the methodologies goes up to an universal approach for GNSS in surface transportation safety-related applications in Section 8.2. Finally, recommendations for further possible researches are introduced in Section 8.3.

8.1 Conclusions

This dissertation considers the formalised GNSS performance properties migration of applying GNSS into train localisation. The GNSS for train localisation should conform both the GNSS QoS and railway RAMS performances. The properties and their definitions are analysed under the same attribute hierarchy based on the service provider standards [22] [4] [131] and user application specifications [133] [64] [18] [20]. The definitions of all the properties are structurally compared. The migration of both performance properties comes to accuracy, reliability, availability, and safety integrity. Accuracy is regarded as the fundamental basis for the other three properties. The reliability, availability, as well as safety integrity are derived according to the accuracy thresholds. This provides the evidence for performance evaluation and verification methodologies of GNSS for train localisation in the following chapters.

The performance evaluation is to demonstrate the quantitative values of GNSS for train localisation in different scenarios. The GNSS receiver location accuracy is evaluated at the first step, this requires a more accurate reference measurement system together to calculate the deviation of each GNSS receiver location. The GNSS receiver locations are divided into three states according to the accuracy levels as: up state, degraded state, and faulty state. The three states make identification of the four properties transformed into state recognition, this makes the performance evaluation in a more formal way. The accuracy evaluation for the up state shows that the trueness is 4.54 meter, the precision is 2.05 meter. The $MTTF$ as the characteristic for reliability property is 184.99 seconds, and the stationary availability is estimated as 82.26%. The dangerous failure rate λ_D is recognised as the characteristic for safety integrity property. From the safety engineering viewpoint, the safety integrity property needs to be analysed according to the functions and operation conditions. Thus different environmental scenarios are analysed for dangerous failure rate. The dangerous failures are determined as exceeding the alarm limit ($\delta_t > d_2$). The open area and the forest environmental scenarios are analysed. The values of the characteristics for the migrated four properties are determined, the values are identified with the proposed GNSS for train localisation specification inherited from the advisories and standards. The identification results shows that only in open area environmental scenario GNSS SPS receiver meets the specification, in other scenarios all performance values are under the request of the specification. So a GNSS SPS receiver only is not enough for train localisation. The other localisation sensors are needed to perform a more reliable and available train localisation function. So a Doppler radar is adopted to form a GNSS-based localisation unit.

The performance verification is then based on the GNSS-based localisation unit. The verification methodology directly benefits from the evaluation values of the GNSS receiver performance for train localisation. In the performance verification process, the reference measurement system is not used any more. The GNSS receiver locations are map-matched to the railway track. The distance between the GNSS receiver location and the map matched location $|D_t|$ is calculated, then the hypothesis testing of $|D_t|$ acceptable on the track is performed. A two layer 2oo2 structure for the GNSS-based localisation unit is designed, the two 2oo2 voting schemes respectively velocity voting and location voting are also using the hypothesis testing methods. With the verification of GNSS receiver location on the track, then the map-matched location on the correct mileage, the safe localisation unit location is delivered for train control purpose.

8.2 Universal Approach

The proposed GNSS for train localisation performance evaluation and verification process is a universal approach. The methodologies can also be applied to other localisation sensors into different means of transportation for the evaluation and verification of other applications (for example: automatic cruise control, automatic vehicle identification, etc.).

The GNSS QoS and railway RAMS terminologies migrated in this dissertation are based on the existing understanding of GNSS requirements, standards, and guidelines either general or application oriented purposes. However, none of the GNSS documents provide appropriate requirements for GNSS in surface transportation safety-related applications. The property migration chapter uses a common attribute hierarchy structure for the GNSS QoS and railway RAMS. This attribute hierarchy representation of the performance is generally applicable for any applications to find the relations and differences between different performance documents. The GNSS for train localisation performance properties and the corresponding characteristics are not only suitable for train localisation but also for road vehicle detections.

The methodologies for GNSS performance evaluation can be regarded as a general evaluation methodology of a certifiable process for GNSS-based safety-related applications in surface transportation. The GNSS receiver location measurements are formally categorised into three states. The characteristics of other properties are formalised according to the states. This makes the evaluation process easy to recognise and apply. Besides, this evaluation process can be expanded with more properties or more characteristics attaching to the proposed evaluation process.

The Petri net model for the GNSS receiver location states is applicable for any location applications. The firing time delay can be studied and fitted into a distribution, the data belonging to a state can be studied and fitted into another distribution. Then the measurements are generalised into different distributions. This gives more possibility for the analysis of the general performance of the measurements.

The whole sequence of define the properties, evaluate the properties, then apply the property values into operation is the natural process of investigating any problems.

8.3 Recommendations

This dissertation has provided considerable baseline for the properties to be evaluated and verified with the purpose of GNSS for train localisation. The characteristics for each property can still be expanded for other GNSS for railway safety-related applications, thus bring more possibilities for GNSS in railway domain.

The main function of the GNSS-based systems in this dissertation is the train localisation. The functions listed in Table 4.2 also show other functions like GNSS receiver location integrity checking and train driving direction determination.

The GNSS receiver location integrity can be evaluated using EGNOS data and other related techniques from the GNSS receiver side. With so many satellites on the sky, it is necessary to use the supplemental satellites and SBAS satellites to provide more integrity and more accuracy from the GNSS side, then the safety integrity of the localisation unit can be assured from GNSS SIS side. The techniques of the combination of the information from the satellites and the information from the GNSS receiver or the localisation unit can be studied to provide a more trustable location measurement.

The driving direction and the track selectivity can be studied with the help of a localisation unit. The performance of the driving direction identification and track selectivity can also be tested in different environmental scenarios. This will improve the localisation unit functionality to a higher level.

The evaluation process for GNSS can be further scandalised as a process for GNSS receivers in various transportation localisation applications. Other legislation and laws need to be investigated to find the requirements for GNSS-based localisation unit for trains. With a complete evaluation based on the standardised evaluation process, the **Sa**tellite-based **L**ocalisation **U**nit for **T**rain (SaLUT) can finally be approved by assessment bodies. This brings SaLUT as a certified system for train localisation.

The evaluation of the environmental scenarios in this dissertation show a glimpse of how the environments affect the quality of the GNSS measurements. The environmental scenarios can be further clearly defined, and the affection of the factors can be identified and then settled to a known constant. With the fixed factors, the testing scenarios can be built. Then the values of the characteristics related to the performance of different GNSS receivers can be easily tested and compared in these determined environmental scenarios. GNSS receivers in extreme environmental scenarios can be tested, the performance of the safety-related functions will be quantified, thus bring the standard of GNSS receiver for safety-related applications testing into reality.

Appendix A

Index of Abbreviations

APOLO **A**dvanced **Po**sition **Lo**cator

APV **A**pproach **P**rocedure with **V**ertical guidance

BDS **B**ei**D**ou Navigation Satellite **S**ystem

CENELEC **C**omité **E**uropéen de **N**ormalisation **Élec**trotechnique

CNTD **C**oordinate based continuous **N**umerical **T**rack **D**escription

DC **D**iagnostic **C**overage

DIN **D**eutsches **I**nstitut für **N**ormung

DOP **D**ilution **O**f **P**recision

ECEF **E**arth **C**entred **E**arth **F**ixed

ECS **E**ddy **C**urrent **S**ensor

E/E/PE **E**lectric/**E**lectronic/**P**rogrammable **E**lectronic

EGNOS **E**uropean **G**eostationary **N**avigation **O**verlay **S**ervice

ERTMS **E**uropean **R**ail **T**raffic **M**anagement **S**ystem

ESA **E**uropean **S**pace **A**gency

ETCS **E**uropean **T**rain **C**ontrol **S**ystem

EU **E**uropean **U**nion

EUC **E**quipment **U**nder **C**ontrol

FA **F**alse **A**larm

FP **F**ramework **P**rogramme

FR **F**ailure **R**ate

FRP **F**ederal **R**adionavigation **P**lan

GBAS **G**round **B**ased **A**ugmentation **S**ystem

GDOP **G**eometric **D**ilution **o**f **P**recision

GIC **G**round **I**ntegrity **C**hannel

GLONASS **Glo**balnaya **Na**vigatsionnaya **S**putnikovaya **S**istema

GNSS **G**lobal **N**avigation **S**atellite **S**ystems

GPS **G**lobal **P**ositioning **S**ystem

GSM-R **G**lobal **S**ystem for **M**obile Communications for **R**ailway

HDOP **H**orizontal **D**ilution **o**f **P**recision

HPL **H**orizontal **P**rotection **L**imit

HR **H**azard **R**ate

ICAO **I**nternational **C**ivil **A**viation **O**rganisation

IEC **I**nternational **E**lectrotechnical **C**ommission

IMU **I**nertial **M**easurement **U**nit

INS **I**nertial **N**avigation **S**ensor

IOC **I**nitial **O**peration **C**apability

IOV **I**n-**O**rbit **V**alidation

ITCS **I**ncremental **T**rain **C**ontrol **S**ystem

KLUB-U Integrated Train Protection System

LAAS **L**ocal **A**rea **A**ugmentation **S**ystem

LPV **L**ocaliser **P**erformance with **V**ertical guidance

MD **M**issed **D**etection

NMEA **N**ational **M**arine **E**lectronics **A**ssociation

MOPS **M**inimum **O**perational **P**erformance **S**tandards

MSI **M**isleading SIS **I**nformation

MTBF **M**ean **T**ime **B**etween **F**ailure

MTTF **M**ean **T**ime **T**o **F**ailure

MTTR **M**ean **T**ime **T**o **R**epair

OBU **O**n-**B**oard **U**nit

PDF **P**robability **D**ensity **F**unction

PDOP **P**osition **D**ilution **o**f **P**recision

PN **P**etri **n**ets

PNT **P**ositioning, **N**avigation, and **T**iming

POI **P**oint **o**f **I**nterest

PRA **P**robabilistic **R**isk **A**ssessment

PTC **P**ositive **T**rain **C**ontrol

QoS **Q**uality **o**f **S**ervice

RAIM **R**eceiver **A**utonomous **I**ntegrity **M**onitoring

RAMS **R**eliability, **A**vailability, **M**aintainability, **S**afety

RBC **R**adio **B**lock **C**entre

RG **R**eachability **G**raph

RMS **R**oot **M**ean **S**quare

RTCA **R**adio **T**echnical **C**ommission for **A**eronautics

RSS **R**oot **S**um **S**quare

RTK **R**eal **T**ime **K**inematic

SARPs **S**tandards **A**nd **R**ecommended **P**ractice**s**

SaLUT **Sa**tellite-based **L**ocalisation **U**nit for **T**rain

SBAS **S**pace **B**ased **A**ugmentation **S**ystem

SIL **S**afety **I**ntegrity **L**evel

SIS **S**ignal **i**n **S**pace

SoL **S**afety **o**f **L**ife

SPN **S**tochastic **P**etri **n**ets

SPS **S**tandard **P**ositioning **S**ervice

TTF **T**ime **t**o **F**ailure

TCC **T**rain **C**ontrol **C**entre

TDOP **T**ime **D**ilution **o**f **P**recision

TOA **T**ime **o**f **A**rrival

UERE **U**ser **E**quivalent **R**ange **E**rror

UML **U**nified **M**odeling **L**anguage

URA **U**ser **R**ange **A**ccuracy

URAE **U**ser **R**ange **A**cceleration **E**rror

URE **U**ser **R**ange **E**rror

URRE **U**ser **R**ange **R**ate **E**rror

USA **U**nited **S**tates of **A**merica

UTCOE **UTC** **O**ffset **E**rror

VDOP **V**ertical **D**ilution **o**f **P**recision

VPL **V**ertical **P**rotection **L**imit

WAAS **W**ide **A**rea **A**ugmentation **S**ystem

WGS **W**orld **G**eodetic **S**ystem

Appendix B

GNSS-based Localisation Unit Hazard Rate Simulation

As introduced in Chapter 7, the GNSS-based localisation is composed by a GNSS receiver and a Doppler radar sensor. The both sensors form a two layer 2oo2 architecture as shown in Figure 7.5. For GNSS-based localisation unit as a safety-related application, it is necessary to undertake the related risk analysis in the localisation unit as required in the system lifecycle [18]. This appendix shows possible ways to estimate the hazard rate of the localisation unit.

The hazard rate is introduced in the dissertation as dangerous undetected rate λ_{DD}. The dangerous undetected failure events are the GNSS receiver deviation $\delta_t \geqslant d_2$, and this is not detected by the localisation unit.

The GNSS receiver locations have been formalised into three states as: up state, degraded state, and faulty state in Chapter 6 Section 6.2. The dangerous undetected faulty are caused by dangerous undetected event. Thus, the dangerous undetected faulty state is part of the faulty state. So the modelled GNSS receiver location states is the basis for the whole localisation unit simulation. The parameters for the transitions in the GNSS receiver location measurement states Petri net model has been evaluated in Chapter 6 Section 6.5. In the localisation unit simulation, it can be directly adopted.

The GNSS receiver velocity and the Doppler radar velocity can also be modelled as the up state, degraded state, and faulty state. But the threshold should be the velocity measurement deviations. With the evaluation of the measured GNSS receiver velocity and the Doppler radar velocity evaluation results, the distribution of the transitions in the Petri net model can also be fitted similar to GNSS receiver location measurements.

The GNSS receiver location with the track-snapping process can derive the acceptance of the GNSS receiver location by real-time verification. The verification algorithm performance shows the dangerous undetected failure rate. Then the faulty state are divided into detected faulty state and undetected faulty state. The entering of the two states are decided by the failure event category. As shown in the dissertation, the GNSS receiver location exceeding the required threshold d_2 is regarded as a dangerous failure event. This is the basic call for other sensors to detect this failure event.

The GNSS receiver velocity and the Doppler radar velocity voting is doing the first layer 2oo2 voting. When both GNSS receiver velocity and Doppler radar velocity are in up state or degraded state, then the voting scheme provides correct voting results. The dangerous failure events exist when both are deliver faulty velocity measurements. Similar to the location measurement, the faulty velocities are also divided into two parts as detected faulty state and undetected faulty state.

The localisation unit dangerous undetected faulty state exist when GNSS receiver location, GNSS receiver velocity, and Doppler radar velocity are all in faulty states, but this situation is not detected, thus the localisation unit is in a hazard state.

The parameters for the GNSS receiver location has been identified by the evaluation of the GNSS receiver location states and the verification of the GNSS receiver location on the track. Using the same methodology, the parameters for the velocity estimation transitions can also be calculated. With all the parameters for the transitions bounded in the dashed boxes as shown in Figure B.1, the hazard rate of the localisation unit can be estimated.

In the combination of up state and degraded state for different measurement component, the localisation unit is delivering safe train location correctly. So they are drawn only one "usable velocity" as an example for all other states. For simplicity of the figure, the other combinations are omitted.

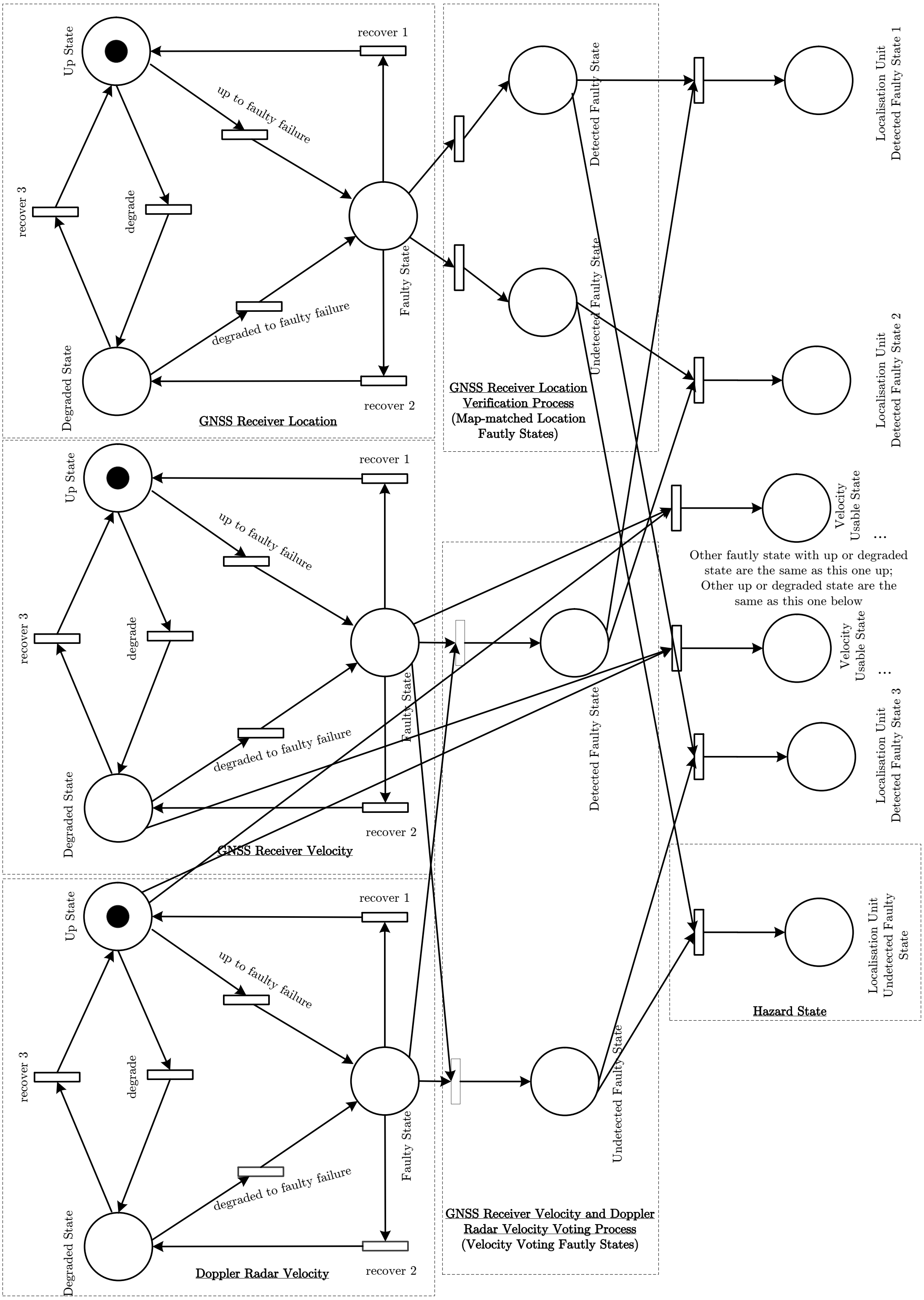


Figure B.1: Localisation Unit Hazard Rate Simulation Petri net Model

Bibliography

[1] Minnie Chan. Beidou launches navigation data for Asia-Pacific region: Satellite navigation network launches tracking data for Asia-Pacific region in warning to GPS. *South China Morning Post*, 28.12.2012. URL `http://www.scmp.com/news/china/article/1113896/beidou-launches-navigation-data-asia-pacific-region`. (checked on 23.10.2013).

[2] Jonathan Amos. Galileo: Europe's version of GPS reaches key phase. *BBC NEWS Science & Environment*, 12.10.2012. URL `http://www.bbc.co.uk/news/science-environment-19933989`. (checked on 23.10.2013).

[3] Xinxin Gao. *Towards Navigation Based on 120 Satellites: Analyzing the New Signals*. PhD thesis, Stanford University, Stanford and California, 2008.

[4] European Commission. Galileo Mission High Level Definition Document (HLD) 3.0, 2002.

[5] European Commission. EGNOS Safety of Life Service Definition Document: EGN-SDD SoL, V1.0, 2011.

[6] Tony Godber. Train Detection Principles. In *IRSE Australasia Technical Meeting*, Melbourne, 2010.

[7] European Union. Directive 2004/50/EC of the European Parliament and of the Council of 29 April 2004: amending Council Directive 96/48/EC on the interoperability of the trans-European high-speed rail system and Directive 2001/16/EC of the European Parliament and of the Council on the interoperability of the trans-European conventional rail system, 2004.

[8] Peter Stanley. *ETCS for engineers*. Eurailpress, Hamburg, 1 edition, 2011. ISBN 978-3-7771-0416-4.

[9] ERTMS Users Group and International Union of Railways. *ETCS Implementation Handbook*. UIC, 2.1 edition, 2008. ISBN 2-7461-1499-2.

[10] Eckehard Schnieder and George Barbu. Potenziale satellitenbasierter Ortung für Eisenbahnen. *ETR - Eisenbahntechnische Rundschau*, 1(Nr. 01+02), 2009.

[11] Eckehard Schnieder. Nutzung von Satellitenortungssystemen für Eisenbahnen im rechtlichen Rahmen: Use of satellite based localisation for railway in legal context. *ZEVrail*, 133(9):351–357, 2009.

[12] International Electrotechnical Commission. IEC 61508-1: Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements, 1997.

[13] International Electrotechnical Commission. IEC 61508-2: Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems, 1997.

[14] International Electrotechnical Commission. IEC 61508-3: Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements, 1997.

[15] International Electrotechnical Commission. IEC 61508-4: Functional safety of electrical/electronic/ programmable electronic safety-related systems — Part 4: Definitions and abbreviations, 1997.

[16] International Electrotechnical Commission. IEC 61508-5: Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels, 1997.

[17] International Electrotechnical Commission. IEC 61508-6: Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of parts 2 and 3, 1997.

[18] European Committee for Electrotechnical Standardization. CENELEC EN 50126: Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), 2007.

[19] European Committee for Electrotechnical Standardization. CENELEC EN 50128: Railway applications - Communications, siganlling and processing systems - Software for railway control and protection systems, 2001.

[20] European Committee for Electrotechnical Standardization. CENELEC EN 50129: Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling, 2003.

[21] Eckehard Schnieder. Qualität dynamischer Satellitenortung im Eisenbahnverkehr. *Technisches Messen*, 4(79 (2012) 4):210–219, 2012. ISSN 0171-8096.

[22] United States Department of Defense. Global Positioning System Standard Positioning Service Performance Standard, 2008. URL `http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf`.

[23] P.J. Cross. A Journey Through Train Detection. In *IRSE Australasia Technical Meeting*, Sydney, 1993.

[24] Dietmar Klimmek. *Modell für die Bewertung von Navigationssystemen im Landverkehr*. PhD thesis, Technische Universität Braunschweig, Braunschweig, 1985.

[25] Dirk Leinhos. *Analyse und Entwurf von Ortungssystemen für den Schienenverkehr mit Strukturierten Methoden*. PhD thesis, Technische Universität Braunschweig, Braunschweig, 1996.

[26] Stefan Hensel. *Wirbelstromsensorbasierte Lokalisierung von Schienenfahrzeugen in topologischen Karten*. PhD thesis, Karlsruher Institut für Technologie (KIT), Karlsruhe, 2011.

[27] Railway Group Standards. General Information on Track Circuits: GK/RC0752, 1998. URL `http://www.rgsonline.co.uk/Railway_Group_Standards/Control%20Command%20and%20Signalling/Codes%20of%20Practice/GKRC0752%20Iss%202.pdf`. (checked on 15.11.2013).

[28] Railway Group Standards. Axel Counters: Code of Practice for Resetting and Restoration to Services: GK/RT0027, 1998. URL `http://www.rgsonline.co.uk/Railway_Group_Standards/Control%20Command%20and%20Signalling/Codes%20of%20Practice/GKRC0527%20Iss%201.pdf`. (checked on 15.11.2013).

[29] Union Industry of Signalling. UNISIG ERTMS/ETCS - Class 1: Fit Functional Interface Specification (FFFIS) for Eurobalise: SUBSET-036, 27.09.2007.

[30] Baigen Cai, Jian Wang, Qin Yin, and Jiang Liu. A GNSS Based Slide and Slip Detection Method for Train Positioning. In *Asia-Pacific Conference on Information Processing*, pages 450–453, Shenzheng, 2009.

[31] Baigen Cai. *Train Integrated Positioning Methods for Low-cost Train Control System*. PhD thesis, Beijing Jiaotong University, Beijing, 2010.

[32] Lei Yuan and Datian Zhou. Error Correction Method for Train Speed Measurement Using Doppler Radar in Train Control System. In *Autonomous Decentralized Systems*, Mexico City, 2013.

[33] Debiao Lu, Federico Grasso Toro, and Eckehard Schnieder. RAMS Evaluation of GNSS for Railway Localisation. In *IEEE International Conference on Intelligent Rail Transportation*, Beijing, 2013.

[34] Aleš Filip, Hynek Mocek, and Lubor Bazant. Zugortung auf GPS/GNSS-Basis für sicherheitskritische Anwendungen. *SIGNAL+DRAHT*, 5:16–21, 2001.

[35] Pierre Mertens, Jean-Pierre Franckart, and Antonin Starck. LOCOPROL: A low cost Train Location and Signalling System for ”Low Density” Lines. In *Proceedings of Word Congress on Railway Research*, Edinburgh, 2003.

[36] Andrew Simsky, Frank Wilms, and Jean-Pierre Franckart. GNSS-based failsafe train positioning system for low-density traffic lines based on onedimensional positioning algorithm. In *2nd ESA Workshop on Satellite Navigation User Equipment Technologies*, Noordwijk, 2004.

[37] Xiaogang Gu. Feasibility of GNSS/Galileo-based train location for safety relevant applications. *SIGNAL+DRAHT*, (97) 1+2:29–34, 2005.

[38] GADEROS: Galileo Demonstrator for Railway Operation System: Project Overview, Project deliverable, 2002.

[39] ECORAIL: GNSS for Safe Railway Road Cross Application: GNSS Applications- Final Presentation, 2006.

[40] A. Albanese and L. Marradi. The RUNE project: the integrity performances of GNSS-based railway user navigation equipment. In *Joint Railroad Conference*, volume 29 of *RTD Ser*, pages 211–218, New York, March 2005. ASME Press. ISBN 0-7918-3752-1.

[41] George Barbu. Railway Geodesy (GEORAIL), 2008. URL `http://www.uic.org/spip.php?article696`. (checked on 15.09.2013).

[42] Bryan Jenkins, Alvaro Urech, and Maria José Garcia Prieto. GNSS Introduction in the RAIL sector. In *The Institution of Engineering and Technology Seminar on Global Navigation Satellite Systems*, pages 143–155, Piscataway and N.J, 2007. IEEE. ISBN 978-0-86341-794-8.

[43] Livio Marradi, Andrea Galimberti, Lucio Foglia, Alberto Zin, Cristina Pecchioni, and Manuel Doronzo. GNSS for Enhanced Odometry: The GRAIL-2 results. In *6th ESA Workshop on Satellite Navigation Technologies : "Multi-GNSS Navigation Technologies Galileo's Here"*, pages 1–7, Noordwijk, 2012. ISBN 978-1-4673-2010-8.

[44] Hansjörg Manz. Galileo Localisation for Railway Operation Innovation (GaLoROI) Project Proposal, 2011.

[45] Jaizki Mendizabal. EATS: ETCS Advanced Testing and Smart Train Positioning System, 2013. URL `http://www.eats-eu.org/index.html`. (checked on 15.11.2013).

[46] Sven Bernhard Kiriczi. *Signaltechnisch sichere Fehlergrenzen für die Erfassung der Bewegungszustände von Bahnen*. PhD thesis, Technische Universität Braunschweig, Braunschweig, 1996.

[47] Karl-Albrecht Klinge. *Konzept eines fahrzeugautarken Ortungsmoduls für den spurgebundenen Verkehr*. PhD thesis, Technische Universität Braunschweig, Braunschweig, 1997.

[48] Gert Bikker and Martin Schroeder. *Methodische Anforderungsanalyse und automatisierter Entwurf sicherheitsrelevanter Eisenbahnleitsystem mit kooperierenden Werkzeugen*. PhD thesis, Technische Universität Braunschweig, Braunschweig, 2002.

[49] Gert Bikker, Uwe Becker, Lorenz Däubler, and Eckehard Schnieder. SATNAB Phase II: Endbericht, 2002.

[50] Jan Poliak. *Validierung von satellitenbasierten Eisenbahnortungssystem*. PhD thesis, Technische Universität Braunschweig, Braunschweig, 2009.

[51] Frank Hänsel. *Zur Formalisierung technischer Normen*. PhD thesis, Technische Universität Braunschweig, Braunschweig, 2008.

[52] Marco Wegener. *Über die metrologische Qualität der Fahrzeugortung*. PhD thesis, Technische Universität Braunschweig, Braunschweig, 2014.

[53] David Shirres. Russian railways shoot for Olympic gold. *The Rail Engineer*, 02.08.2012. URL `http://www.therailengineer.com/2012/08/02/russian-railways-shoot-for-olympic-gold/`. (checked on 08.03.2013).

[54] Izhevskiy Radiozavod. Unified Integrated Locomotive Safety System KLUB-U, 2013. URL `http://en.irz.ru/products/20/70.htm`. (checked on 08.03.2013).

[55] Patrick Jarvis. GE Wins Order From Chinese Ministry of Railways for 78 Locomotives Second Contract Awarded for Incremental Train Control System, 2005. URL `http://www.getransportation.com/rail/rail-products/signaling-a-communication/signaling-a-train-control/incremental-train-control-system-itcs.html`. (checked on 21.09.2010).

[56] Greg Hann. Incremental Train Control System. *IEEE Vehicular Technology Magazine*, 5(4):50–55, 2010. doi: 10.1109/MVT.2010.939108.

[57] Michael Schabas. Eko Rail wins Lagos Blue Line concession. *Metro Report International*, 3, 2012.

[58] Bob Pemberton. Leveraging New Technology to Create Higher Capacity Networks. In *International Railway Safety Conference*, Melbourne, 2011.

[59] Burkhard Stadlmann. Zugleitsystem für Regionalstrecken. In *INFORMATIK*, 2003.

[60] Burkhard Stadlmann. GPS Based Train Control System in Austria. In *ZEL-GNSS WORKSHOP*, Zilina, 2008.

[61] Liesbeth de Jong. UIC launches SATLOC, a new EU funded project for the development of satellite based operation of local low rail traffic lines, 13.02.2012. URL `http://www.uic.org/com/IMG/pdf/cp_uic_launches_satloc_en-2.pdf`. (checed on 12.06.2013).

[62] Mike Agron. GNSS Performance Standards & Certification Beyond Spectrum Protection. Inside GNSS: Prensentation Slides, 2013.

[63] Radio Technical Commission for Aeronautics. RTCA DO-208: Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment Using Global Positioning System (GPS), 1991.

[64] Radio Technical Commission for Aeronautics. RTCA DO-229D: Minimum Operational Performance Standards for Global Positioning System/Wide Area Augmentation System Airborne Equipment, 2006.12.13.

[65] Radio Technical Commission for Aeronautics. RTCA DO-253C: Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment, 2008.12.16.

[66] Sam Pullen, Todd Walter, and Per Enge. SBAS and GBAS Integrity for Non-Aviation Users: Moving Away from "Specific Risk". In *International Technical Meeting of the Institute of Navigation*, pages 533–545, San Diego, 2011.

[67] Aleš Filip, Hynek Mocek, and A. Suchanek. Significance of the Galileo Signal-in-Space Integrity and Continuity for Railway Signalling and Train Control. In *Proceedings of Word Congress on Railway Research*, Paris, 2008.

[68] Aleš Filip. A Relation among GNSS Quality Measures and Railway RAMS Attributes. In *CERGAL*, Braunschweig, 2008.

[69] Aleš Filip, Julie Beugin, Juliette Marais, and Hynek Mocek. Interpretation of the Galileo Safety-of-Life Service by Means of Railway RAMS Terminology. *Transactions on Transport Sciences*, 1(2):61–68, 2008. ISSN 1802-971X.

[70] The Institute of Navigation. ION STD 101 Recommended Test Procedures For GPS Receivers, 1997.

[71] Aleš Filip. Which of EGNOS Navigation Modes for Railway Siganlling: Precision Approach or En Route? In *CERGAL*, Rostock, 2010.

[72] Aleš Filip, Lubor Bazant, and Hynek Mocek. The experimental evaluation of the EGNOS safety-of-life services for railway signalling. In *COMPRAIL*, Beijing, 2010.

[73] Julie Beugin and Juliette Marais. Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization. *Transportation Research Part C: Emerging Technologies*, 22:42–57, 2012. ISSN 0968090X. doi: 10.1016/j.trc.2011.12.002.

[74] Patrick Y. HWANG and R. Grover Brown. From RAIM to NIORAIM: A New Integrity Approach to Integrated Multi-GNSS Systems. *Inside GNSS*, 3: 24–33, 2008.

[75] David M. Bevly. *GNSS for Vehicle Control*. GNSS technology and applications series. Artech House, Boston, 2010. ISBN 1596933011.

[76] Young C. Lee. Analysis of Range and Position Comparison Methods as a Means to Provide GPS Integrity in the User Receiver. In *Proceedings of the 42th Annual Meeting of the Institute of Navigation*, Seattle, 1986.

[77] Bradford W. Parkinson and Penina Axelrad. Autonomous GPS Integrity Monitoring Using the Pseudorange Residual. *NAVIGATION: Journal of the Institute of Navigation*, 35(2):255–274, 1988. ISSN 0028-1522.

[78] Boris S. Pervan, David G. Lawrence, Clark E. Cohen, and Bradford W. Parkinson. Parity Space Methods for Autonomous Fault Detection and Exclusion using GPS Carrier Phase. In *IEEE/ION PLANS*, pages 649–656, Atlanta, 1996. ISBN 0-7803-3085-4.

[79] R. Grover Brown. A Baseline RAIM Scheme and a Note on the Equivalence of Three RAIM Methods. *NAVIGATION: Journal of the Institute of Navigation*, 39(3):301–316, 1992. ISSN 0028-1522.

[80] Igor V. Nikiforov. Integrity Equation for Safe Train Positining Using GNSS. In *ENC GNSS*, Graz, 2003.

[81] Eckehard Schnieder, Karl-Albrecht Klinge, and Gert Bikker. RailOrt - Ortung um spurgebunden Verkehr auf der Basis von Satelliten-Navigation: Project Report, 2001.

[82] Adrian Waegli, Stéphane Guerrier, and Jan Skaloud. Redundant MEMS-IMU integrated with GPS for Performance Assessment in Sports. In *IEEE/ION PLANS*, pages 1260–1268, Monterey, 2008.

[83] Jiang Liu, Tao Tang, Baigen Cai, Jian Wang, and DeWang Chen. Integrity assurance of GNSS-based train integrated positioning system. *Science China Technological Sciences*, 54(7):1779–1792, 2011. ISSN 1674-7321. doi: 10.1007/s11431-011-4395-z.

[84] Jana Heckenbergerova. GNSS Train Position Integrity Monitoring by the help of discrete PIM algortihms. *Journal of Applied Mathematics*, 2(3):73–80, 2009.

[85] Grady Booch, James Rumbaugh, and Ivar Jacobson. *The unified modeling language user guide*. The Addison-Wesley object technology series. Addison-Wesley, Reading Mass, 1999. ISBN 0201571684.

[86] Deutsches Institut für Normung. DIN 2342: Begriffe der Terminologielehre, 2011.08.

[87] Lars Schnieder. *Formalisierte Terminologien technischer Systeme und ihrer Zuverlässigkeit*. PhD thesis, Technische Universität Braunschweig, Braunschweig, 2010.

[88] Hansjörg Manz, Lars Schnieder, Matthias Hübner, and Eckehard Schnieder. Modeling of domain spanning technologies for satellilite based localization systems by specifying terminologies. In *IAIN*, Stockholm, 2009.

[89] Marco Wegener, Matthias Hübner, and Eckehard Schnieder. Anforderungen an ein Referenzmesssystem zur Untersuchung der GPS-Messqualität. *Technisches Messen*, 78(7-8):354–363, 2011. ISSN 0171-8096. doi: 10.1524/teme.2011.0199.

[90] Felix Reinbold, Marco Wegener, and Eckehard Schnieder. QualiSaR - Development of a Qualification Procedure for the Usage of Galileo Satellite Receivers for Safety Relevant Applications. In *ENC GNSS*, Gdańsk, 2012.

[91] Jörg Rudolf Müller. Die formalisierte Terminologie der Verlässlichkeit technischer Systeme: Habilitationsschrift, 2012.

[92] Rudolf Carnap. *Physikalische Begriffsbildung. Wissenschaftliche Buchgesellschaft*. Philosophische Bibliothek. Felix Meiner, Darmstadt, 1966.

[93] International Electrotechnical Commission. IEC 19505-1: Information technology – Object Management Group Unified Modeling Language (OMG UML) – Part 1: Infrastructure, 2012.

[94] Eckehard Schnieder. *Verkehrsleittechnik: Automatisierung des Straßen- und Schienenverkehrs*. Springer, Berlin, 2007. ISBN 3540482962.

[95] Eckehard Schnieder. *Methoden der Automatisierung: Beschreibungsmittel, Modellkonzepte und Werkzeuge für Automatisierungssysteme*. Vieweg Verlagsgesellschaft, Wiesbaden, 1999. ISBN 3528065664.

[96] Verein Deutscher Ingenieure. VDI 4004-5: Leitfaden zur formalisierten Begriffsmodellierung zentraler Termini der technischen Zuverlässigkeit, 2012.

[97] Esther Schmalkuche. iglos User Manual, 2014.

[98] Carl Adam Petri. *Kommunikation mit Automaten*. PhD thesis, Technische Universiät Darmstadt, Darmstadt, 1962.

[99] Winfrid G. Schneeweiss. *Petri nets for reliability modeling: (in the fields of engineering safety and dependability) // Petri nets for reliability modeling: In the fields of engineering safety and dependability*. LiLoLe-Verlag, Hagen, 1999. ISBN 3934447007. URL `http://www.worldcat.org/oclc/43337111`.

[100] Carl Adam Petri. Nets, time and space. *Theoretical Computer Science*, 153 (1-2):3–48, 1996. ISSN 03043975. doi: 10.1016/0304-3975(95)00116-6.

[101] Claude Girault and R. Valk. *Petri nets for systems engineering: A guide to modeling, verification, and applications*. Springer, New York, 2003. ISBN 978-3-540-41217-5.

[102] Gustavo Callou, Paulo Maciel, Dietmar Tutsch, Julian Arajo, Joo Ferreira, and Rafael Souz. A Petri Net-Based Approach to the Quantification of Data Center Dependability. In Pawel Pawlewski, editor, *Petri Nets - Manufacturing and Computer Science*. InTech, 2012. ISBN 978-953-51-0700-2. doi: 10.5772/47829.

[103] Falko Bause and Pieter S. Kritzinger. *Stochastic Petri nets: An introduction to the theory*. Advanced studies in computer science. Vieweg, Wiesbaden, 2nd edition, 2002. ISBN 3528155353.

[104] Sheldon M. Ross. *Stochastic processes.* Wiley series in probability and statistics. Probability and statistics. Wiley, New York, 2nd edition, 1996. ISBN 0471120626.

[105] Morris H. DeGroot. *Probability and statistics.* Addison-Wesley series in statistics. Addison-Wesley, Reading Massachusetts, 2nd edition, 1986. ISBN 020111366x.

[106] Bernd Bertsche and Gisbert Lechner. *Zuverlässigkeit im Fahrzeug- und Maschinenbau: Ermittlung von Bauteil- und System-Zuverlässigkeiten.* VDI-Buch. Springer, Dordrecht, 3rd edition, 2004. ISBN 978-3-540-34996-9.

[107] Marvin K. Simon. *Probability distributions involving Gaussian random variables: A handbook for engineers, scientists and mathematicians.* Springer, New York and NY, 1. softcover printing edition, 2006. ISBN 1402070586.

[108] Frederick J. Gravetter and Larry B. Wallnau. *Statistics for the behavioral sciences.* Wadsworth, Belmont and CA, 8th edition, 2009. ISBN 0495602205.

[109] E. L. Lehmann and Joseph P. Romano. *Testing statistical hypotheses.* Springer texts in statistics. Springer, New York, 3rd edition, 2005. ISBN 0-387-98864-5.

[110] Josef Börcsök. *Functional safety: Basic principles of safety-related systems.* Practice. Hüthig, Heidelberg, 2007. ISBN 3778529862.

[111] Josef Börcsök. *HIMA dictionary of safety-related technology.* VDE-Verlag, Berlin, 2011. ISBN 9783800733170. URL `http://www.worldcat.org/oclc/703891282`.

[112] Mohamed Mahmoud. Performance and QoS: Lecture Slides, 2013.

[113] Niels Klußmann and Arnim Malik. Lexikon der Luftfahrt. *Lexikon der Luftfahrt*, 2012.

[114] Noah Webster. *The Merriam-Webster dictionary.* Merriam-Webster, Springfield and Mass, 2005. ISBN 087779636X.

[115] European Railway Agency. ERTMS/ETCS Functional Requirements Specification FRS: ERTMS/ETCS FRS v 5.00, 2007.

[116] Bernhard Hofmann-Wellenhof, Klaus Legat, and Manfred Wieser. *Navigation: Principles of Positioning and Guidance.* Springer Vienna, Vienna, 2003. ISBN 9783211008287.

[117] Mohinder S. Grewal, Angus P. Andrews, and Chris G. Bartone. *Global Navigation Satellite Systems, Inertial Navigation, and Integration.* John Wiley & Sons Inc, New York, 3 edition, 2013. ISBN 978-1-118-44700-0.

[118] Charles Jeffrey. *An Introduction to GNSS: GPS, GLONASS, Galileo and other Global Navigation Satellite Systems.* NovAtel Inc., Calgary, 1st edition, 2010. ISBN 978-0-9813754-0-3.

[119] Sterling Udell. *Beginning Google Maps mashups with mapplets, KML, and GeoRSS: From novice to professional*. The expert's voice in web development. Apress and Distributed by Springer-Verlag New York, Berkeley and CA and New York and NY, 2009. ISBN 9781430216209.

[120] Andreas Heckmann and Sebastian Streit. The Modeling of Energy Flows in Railway Networks using XML-Infrastructure Data. In *9th International MODELICA Conference*, pages 125–132, Munich, 2012.

[121] Jürgen Beyer. Contribution to Safety Relevant Navigation: New Analytical Approach towards Optimal Data Fusion: am Institut für Meß- und Regeltechnik der Eidgenössische Hochschule ETH in Zürich, 1998.

[122] ERTMS Users Group. ODOMETER Form Fit Functional Interface Specification (FFFIS): EEIG 97E267, 1998.

[123] Jan Poliak, Juliette Marais, and Frank Hänsel. Validation Process for Usage Galileo in Railways. In *Proceedings of the 15th International Symposium Eurnex - Zel 2007 "Towards the competetive rail system in Europe"*, Zilina, 2007.

[124] Elliott D. Kaplan and Christopher J. Hegarty. *Understanding GPS: Principles and applications // Understanding GPS: Principles and applications*. Artech House, Boston and Mass, 2nd edition, 2006. ISBN 9781580538947. URL `http://www.worldcat.org/oclc/803725789`.

[125] Harry Evers and Günther Kasties. *Kompendium der Verkehrstelematik: Technologien, Applikationen, Perspektiven*. Vlg. TÜV Rheinland, Köln, 1998. ISBN 3824904217.

[126] Paul D. Groves. *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*. GNSS technology and application series. Artech House, Boston, 2nd edition, 2013. ISBN 1608070050.

[127] Pratap Misra and Per Enge. *Global positioning system: Signals, measurements, and performance*. Ganga-Jamuna Press, Lincoln and Mass, 2nd edition, 2011. ISBN 0970954425.

[128] Richard B. Langley. NMEA 0183: A GPS Receiver Interface Standard. *GPS World*, July(July), 1995.

[129] European Commission. EGNOS Service Definition Document Open Service, 2009.

[130] European Commission. New European satellite navigation service increases aviation safety, 02.03.2011. URL `http://europa.eu/rapid/press-release_IP-11-247_en.htm?locale=en`. (checked on 16.02.2013).

[131] European Commission. EGNOS Safety of Life Service Definition Document: EGNOS SDD SoL, 2013.

[132] Erwin Lassooij. Overview of APV: ICAO EUR APV Workshop: Slides, 2010. URL `https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CC0QFjAA&url=http%3A%2F%2Fwww.paris.icao.int%2Fdocuments_open_meetings%2Fdownload.php%3Fmaincategory%3D84%26subcategory%3D86%26file%3DDay3_1_ICAO.pdf`. (checked on 15.11.2013).

[133] United States Department of Defense, United States Department of Homeland Security, and Department of Transportation. 2010 Federal Radionavigation Plan: DOT-VNTSC-RITA-08-02/DoD-4650.05, 2010.

[134] International Civil Aviation Organization. ICAO Annex 10 to the Convention on International Civil Aviation: Aeronautical Telecommunications, Volume 1, Radio Navigation Aids, 2006.

[135] George Barbu, J-M Wiss, P Frosig, M Schröder, K Walter, Aleš Filip, A Sage, and S Forsyth. GNSS Rail User Forum: Requirements of Rail Applications, 2000.

[136] International Electrotechnical Commission. IEC 60050-191: International Electrotechincal Vocabulary (IEV) - part 191: Dependability and Quality of Service, 2002.

[137] International Organization for Standardization. ISO/IEC Guide 51: Safety aspects - Guidelines for their inclusion in standards, 2012.

[138] International Electrotechnical Commission. IEC 60300: International standards on dependability, 2006.

[139] Marvin Rausand and Arnljot Høyland. *System reliability theory: Models, statistical methods, and applications*. Wiley series in probability and statistics. Applied probability and statistics. Wiley-Interscience, Hoboken and NJ, 2nd edition, 2004. ISBN 047147133X.

[140] Morris Chudleigh. Risk Analysis and Mitigation: Presentation to MHRA: Presentation Slides, 2010.

[141] Debiao Lu, Daohua Wu, and Eckehard Schnieder. Hazard Analysis for GNSS-based Train Localisation Unit with Model Based Approach According to EGNOS and Railway RAMS. In *IAIN*, Cairo, 2012.

[142] Marco Wegener and Eckehard Schnieder. Application of the GUM method for state-space systems in the case of uncorrelated input uncertainties. *Measurement Science and Technology*, 24(2):025003, 2013. ISSN 0957-0233. doi: 10.1088/0957-0233/24/2/025003.

[143] Jürgen Beyer. Regelungstechnische Ansätze zur Steigerung der Betriebsqualität und Trassenkapazität im Eisenbahnverkehr: Regelungstechnisches Kolloquium an der RWTH Aachen, 2008.

[144] International Electrotechnical Commission. IEC 62551: Analysis techniques for dependability – Petri net modelling, 2012.

[145] Roman Slovak. *Methodische Modellierung und Analyse von Sicherungssystem des Eisenbahnverkehrs*. PhD thesis, Technische Universität Braunschweig, Braunschweig, 2006.

[146] James D. Hamilton. *Time series analysis*. Princeton University press, Princeton and N.J, 1994. ISBN 0691042896.

[147] European Space Agency. User Guide for EGNOS Application Developers, 2009.

[148] DLR. *Entwicklung eines Demonstration für Ortungsaufgaben mit Sicherheitsverantwortung im Schienengüterverkehr: DemoOrt. Abschlussbericht der Phasen 1 und 2*. DLR, Braunschweig, 2009. ISBN ISSN 1866-721X.

[149] Uwe Becker, Jan Poliak, Alexander Geistler, Carsten Hasberg, and Michael Meyer zu Hörste. DemoOrt repositions trains with satellite. *EURAILmag Business & Technology*, 18:216–219, 2008.

[150] Debiao Lu, Hansjörg Manz, Jörg Rudolf Müller, and Eckehard Schnieder. Integrity Verification for Satellite based Train Localisation Unit Structure by Means of Petri net. In *ENC GNSS*, London, 2011.

[151] Liyan Li, Jie Zhong, and Minjian Zhao. Doppler-Aided GNSS Position Estimation with Weighted Least Squares. *IEEE Transactions on Vehicular Technology*, 60(8):3615–3624, 2011. ISSN 0018-9545. doi: 10.1109/TVT.2011.2163738.